Oracle® MICROS Simphony First Edition

PA-DSS 3.2 Implementation Guide

Release 1.8.x.x
F22931-01
August 2020

Oracle® MICROS Simphony First Edition PA-DSS 3.2 Implementation Guide, Release 1.8.x.x

F22931-01

Contents

Preface

This document describes the steps that you must follow in order for your Simphony First Edition installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016). You can download the PCI PA-DSS 3.2 Requirements and Security Assessment Procedures from the PCI SSC Document Library.

Oracle® MICROS instructs and advises its customers to deploy Oracle® MICROS applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, you should follow the best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various benchmarks, in order to enhance system logging, reduce the chance of intrusion, increase the ability to detect intrusion, and other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling infrequently-used or frequently vulnerable networking protocols, and implementing certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this Implementation Guide in order for your Simphony First Edition installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
August 2020	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 Food and Beverage documentation page on the Oracle Help Center at https://docs.oracle.com/en/industries/food-beverage/ to view or download the current version of this guide, and refer to the Simphony First Edition'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 https://www.oracle.com/technetwork/topics/security/alerts-086861.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 Simphony First Edition in a PCI DSS compliant manner.

1 Executive Summary

Simphony First Edition 1.8.x.x has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc.	Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450,	1633 Westlake Ave N #100
Westminster, CO 80021	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® MICROS Simphony First Edition Version 1.8.x.x as a PA-DSS validated application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs:

- 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">Simphony First Edition</td><td>Payment Application Version</td><td colspan="2">1.8.x.x</td></tr>
<tr><td>Payment Application Description</td><td colspan="5">Simphony First Edition 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 First Edition is capable of operating multiple types of concepts within each property including table service, fast casual, and retail. Simphony First Edition is a payment application designed for the food and beverage and retail industries.</td></tr>
<tr><td>Typical Role of the Payment Application</td><td colspan="5">Simphony First Edition 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): Food and Beverage</td></tr>
<tr><td rowspan="3">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, store cardholder data:
SECURE_DETAIL
CCBATCH_DETAIL
CCBATCH_AUTH_DETAIL
GUEST_CHECK_LINE_ITEM
POS_JOURNAL_LOG
QUE_CHECKS
QUE_CHECKS_HIST
QUE_CHECKS_INPROC
QUE_CHECKS_RETRY
WS_OTF
Guest Check file
Offline transaction file</td><td colspan="2">The following Cardholder data is stored:
Full PAN
Cardholder Name
Expiration date
Last 4 digits of Account Number
Authorization Code</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>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></td><td colspan="5">POS Operations (SAROps)
Service Host (Credit Card processor and communications driver)
EMC – Configuration, Credit Card Batching & Settlement
EGateway – Batch Settlement</td></tr>
</table>

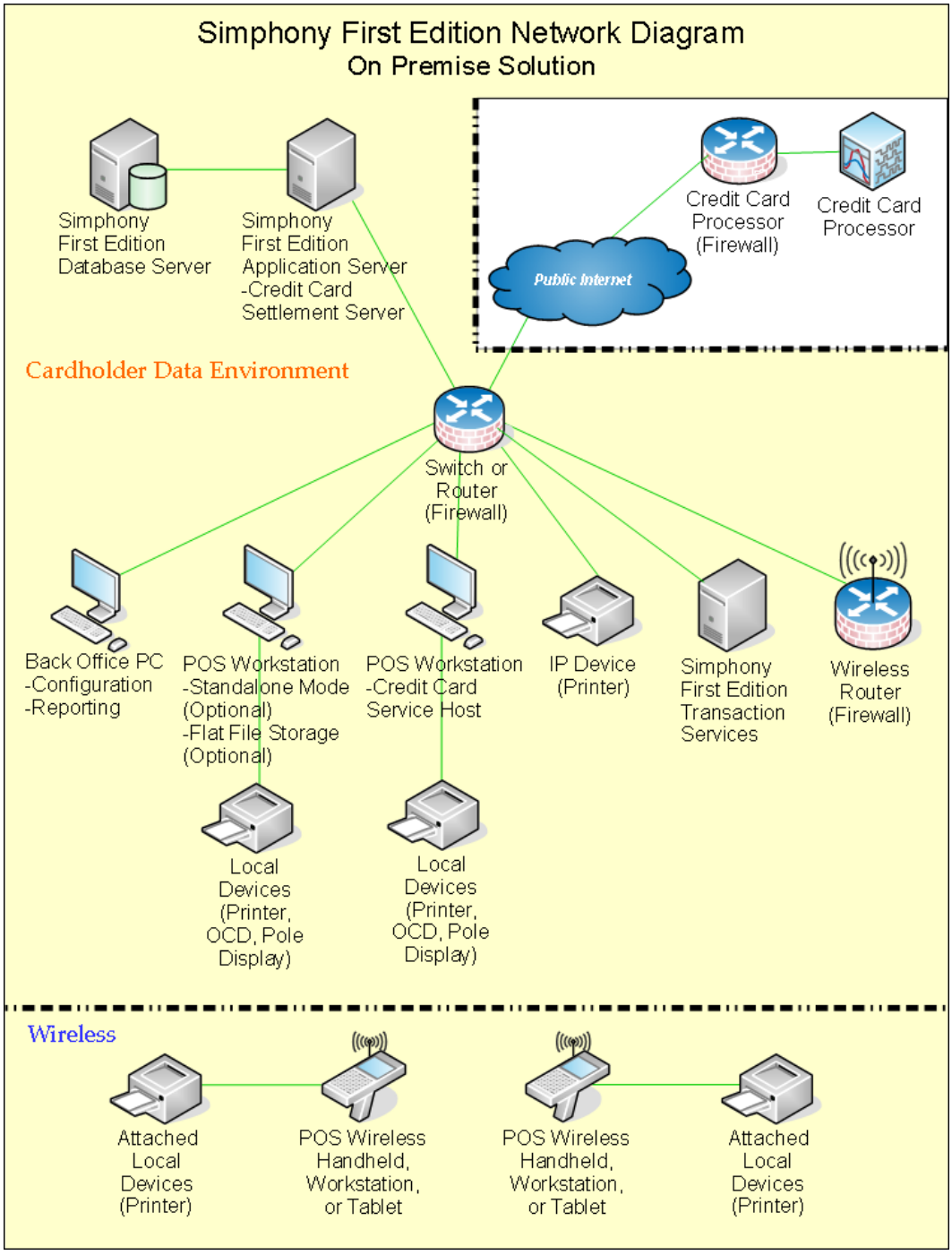
	• Transaction Services • Reporting and Analytics (formerly mymicros.net) – Credit Card Reports
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application:
	None.
Supported Database Software	The following are database management systems supported by the payment application:
	• Oracle Database 12c • Oracle Database 11g • Microsoft SQL Server 2016
Other Required Third Party Software	The following are other third party software components required by the payment application:

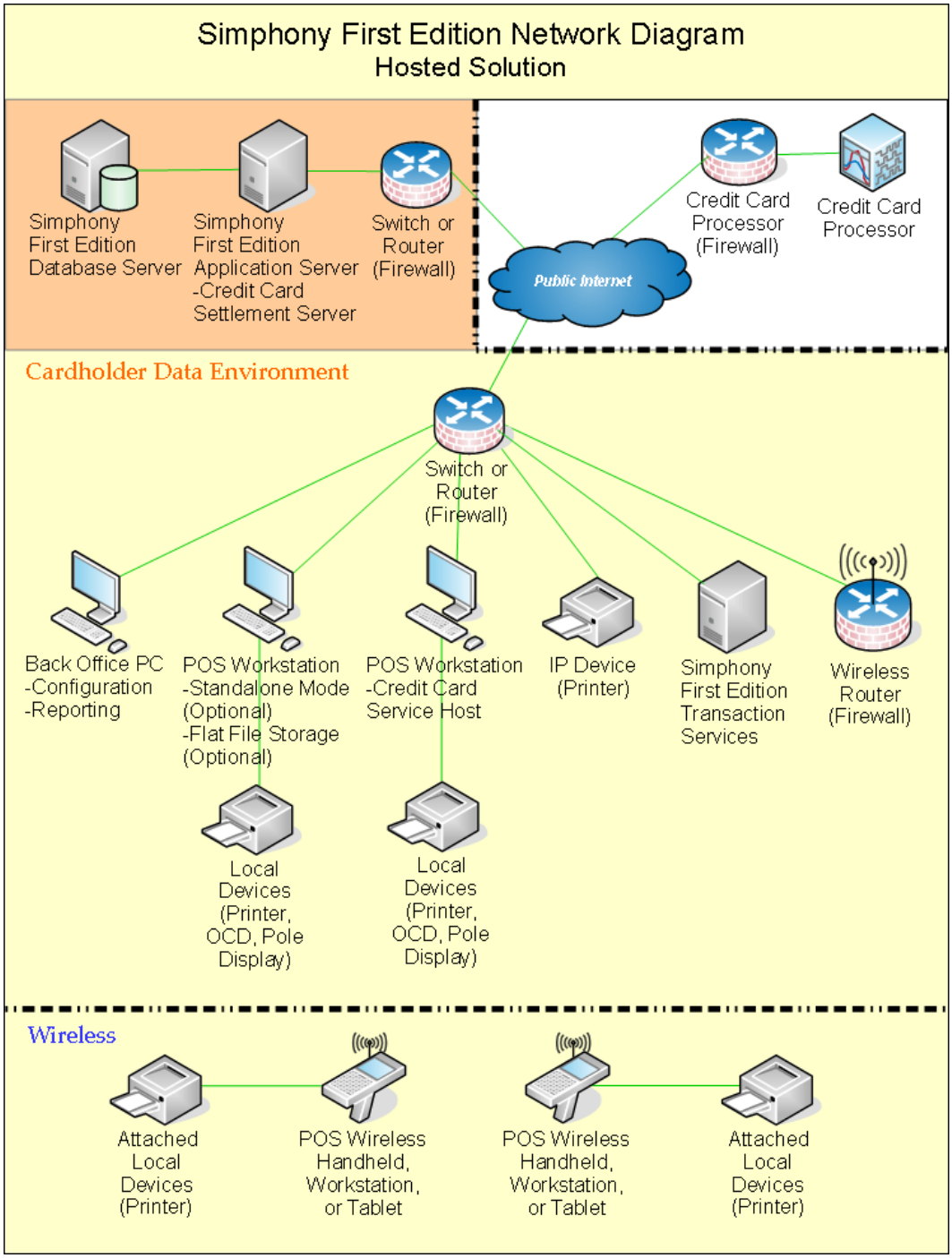
	• For Microsoft Windows Server 2016
	  o Microsoft Internet Information Systems (IIS) version 10
	• For Microsoft Windows Server 2012 R2
	  o Microsoft Internet Information Systems (IIS) version 8.5
	  IIS is used by the payment application to communicate via the web with network clients.
	• WebLogic – version 11g 10.3.6.0
	  WebLogic is used by the Back Office Reporting and Analytics reports application.
	• Microsoft .NET Framework 4.6.2

Supported Operating System(s)	The following are Operating Systems supported or required by the payment application:
	• Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows Embedded POSReady 7 • Microsoft Windows Embedded Compact • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Oracle Enterprise Linux versions 6.x (database servers only)
Payment Application Authentication	**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 The passwords is hashed using SHA 256 and then stored in the database.

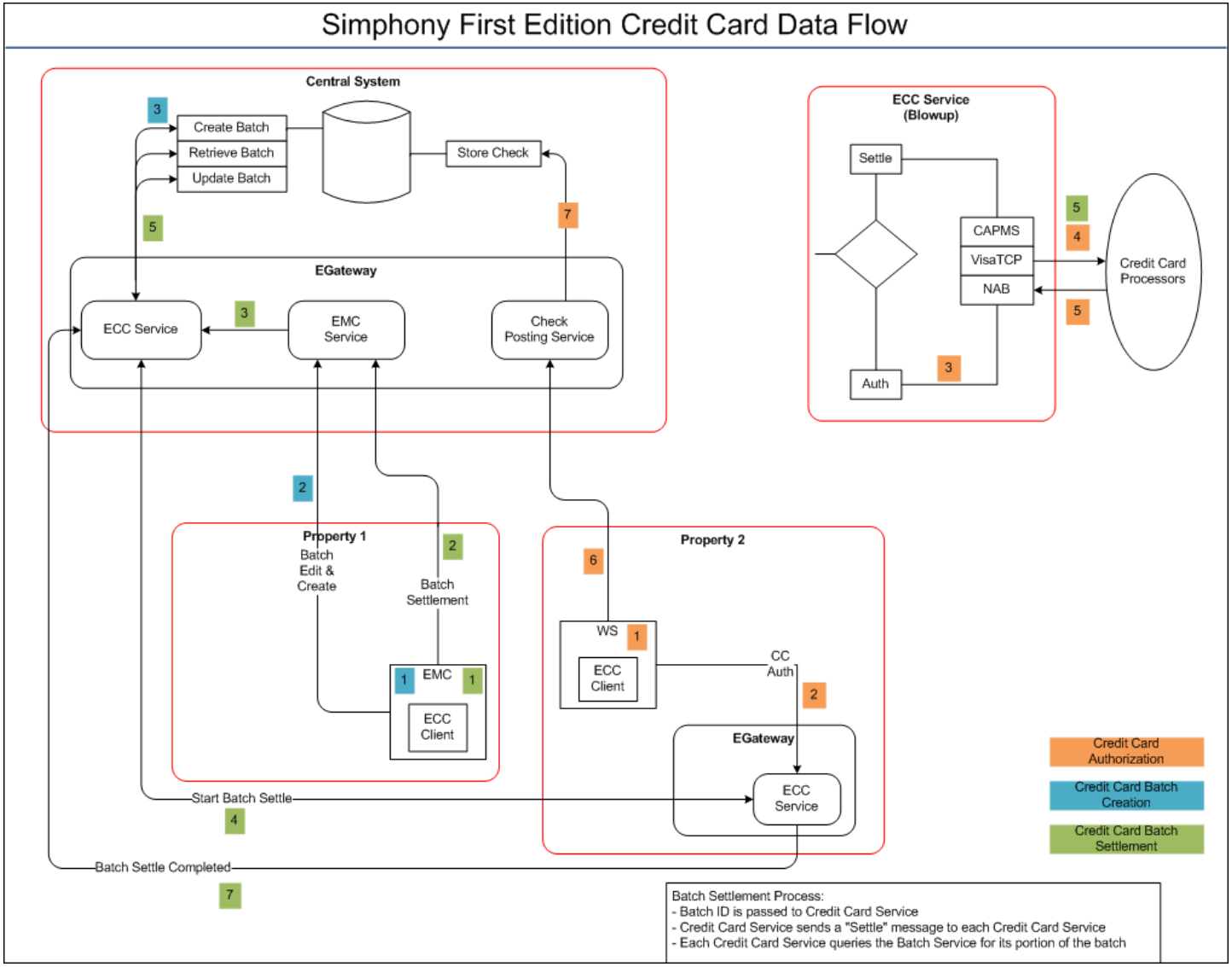
Payment Application Encryption	See page A-1 in Appendix A for information about the payment application encryption used by Simphony First Edition version					
Supported Payment Application Functionality	☐	Automated Fuel Dispenser	☒	POS Kiosk	☐	Payment Gateway/ Switch
	☒	Card-Not-Present	☐	POS Specialized	☐	Payment Middleware
	☐	POS Admin	☐	POS Suite/General	☒	Payment Module
	☒	POS Face-to-Face/POI	☐	Payment Back Office	☐	Shopping Card & Store Front
Payment Processing Connections	Encrypted cardholder data is transmitted from the POS workstation to the on property credit card service machine. The cardholder data in unencrypted and sent to the credit card processor using TCPIP over a secure connection. The credit card processor returns an authorization code to the credit card service machine which is then returned to the POS workstation. The payment details are then forwarded to the enterprise application server and stored in the database until the settlement process is executed. Nightly credit card batches are created and transmitted to the credit card processor via TCPIP using a secure connection.					
Description of Listing Versioning Methodology	Oracle implements wildcard versioning and follows a versioning methodology for the application in the format of [N].[N].[N].[N] (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. Additional hardware platform and OS support can be added at the Minor level that may result in high level impact to PA-DSS requirements. • Changes at the Patch level include one or more changes made at the Interim level, and do not impact PA-DSS requirements or the security of the application. • Changes at the Interim level do not impact PA-DSS requirements or the security of the application. The versions of the payment application listed on the PCI SSC web site are listed as Major.Minor.X.X.					

Typical Network Implementation




Simphony First Edition Network Diagram
Hosted Solution
Simphony First Edition Database Server
Simphony First Edition Application Server -Credit Card Settlement Server
Switch or Router (Firewall)
Public Internet
Credit Card Processor (Firewall)
Credit Card Processor
Cardholder Data Environment
Switch or Router (Firewall)
Back Office PC -Configuration -Reporting
POS Workstation -Standalone Mode (Optional) -Flat File Storage (Optional)
POS Workstation -Credit Card Service Host
IP Device (Printer)
Simphony First Edition Transaction Services
Wireless Router (Firewall)
Local Devices (Printer, OCD, Pole Display)
Local Devices (Printer, OCD, Pole Display)
Wireless
Attached Local Devices (Printer)
POS Wireless Handheld, Workstation, or Tablet
POS Wireless Handheld, Workstation, or Tablet
Attached Local Devices (Printer)

Credit/Debit Cardholder Dataflow Diagram



Credit Card Authorization

1. Credit card data is entered into the Simphony First Edition Point-of-Sale (POS) workstation in the following ways:
    a. Operator manually enters the account number and expiration date.
    b. An unencrypted Mag Stripe Reader (MSR) generates raw track data.

    The POS workstation may request additional information such as the Address Verification System (AVS) or the Card Verification Value (CVV).
2. The authorization request message is formatted by the workstation and sent to the EGateway web service running on the Credit Card Service machine. This communication is AES-256 encrypted, over HTTPS. Credit Card Service machines can be located either at the store, or in the central hosting center. In the former case, communication will occur over the local LAN. In the latter case, communication will be over the WAN or Internet.
3. The Credit Card Service reformats the request and sends it to the credit card processor via TCP/IP. These messages are unencrypted, but are transmitted over either a secure VPN connection, or HTTPS using TLS.
4. The response comes back from the processor over the same connection. During this period the credit card data including the PAN is storing in the Server's RAM.
5. The Credit Card Service reformats the response and sends it back to the workstation. This is encrypted and transmitted as specified above in step 2.
6. The workstation formats the cardholder information and response into the guest check structure. The check is then written locally into a AES-256 encrypted file. It is also transmitted via the mechanism in step 2 to the Check and Posting Service running in the central hosting center.
7. The Check and Posting Service writes the check to the transactional database, encrypting the credit card information using AES-256. The communication between the Check and Posting Service and the database is expected to be a secure layer implemented by the database vendor. During this process the credit card data including the PAN is held in the Server's RAM and cleared immediately when processing has completed.

Credit Card Batch Creation

1. User launches EMC and chooses option to create a batch.
2. EMC sends a message to the EMC Service running in the hosting center. This message contains no sensitive data.
3. EMC Service calls the Credit Card Service locally, which reads the checks with credit cards on them from the database, then writes back a credit card detail record. Communication is expected to be secure, as in step 7 above. During this process the CC data is maintained in RAM memory, it is cleared when processing has been completed.

Credit Card Batch Settlement

1. User launches EMC and chooses a batch to settle.
2. EMC sends a message to the EMC Service running in the hosting center. This message contains no sensitive data.

3. The EMC Service sends a message to the Credit Card Service (either located in the store, or located in the hosting center). This message contains no sensitive data.
4. The Credit Card Service requests batch records from the Credit Card Service located in the hosting center (which may be the same Credit Card Service). This request contains no sensitive data.
5. The hosting center Credit Card Service reads the record from the database, decrypts them, formats a response message, and then sends it back to the Credit Card Service which is doing the settling. This message is encrypted and transmitted in the same manner as the web service messages above.
6. For each record in the batch, the Credit Card Service reads the CC data into RAM, formats a batch transfer request, then sends it to the processor and waits for the response. The CC data is then erased from memory. This communication occurs in the same manner as a credit card authorization, and includes much of the same data.
7. The Credit Card Service settling the batch asks the host Center Credit Card Service to mark the record as transferred. There is no sensitive data in this message.

Credit Card Batch Reporting

1. On a periodic schedule, the Data Transfer Service (New DTS) looks for credit card batch entries which have been transferred.
2. The Data Transfer Service reads the entries from the transaction database, decrypts them, masks all sensitive data, then writes the entry to the reporting database. As above, encryption of data over database connections is done by the database vendor.

Credit/Debit Stored Cardholder Data

Data Store	Cardholder Data Elements stored	How the Data Store is secured	How is access to Data Store logged
• MCRSPOS database SECURE_DETAIL table • QUE_CHECKS • QUE_CHECK_HIST • QUE_CHECK_INPROC • QUE_CHECKS_RETRY • WS_OTF	Primary Account Number (PAN) depending if manual or swipe entry Cardholder name[1] Expiration Date Auth Code Last 4 digits of account number	AES-256 encryption using RSA 2048 bit key pairs	Access to this table is logged by database auditing tools
• MCRSPOS database • CCBATCH_DETAIL table	Auth Code	Plain Text	Access to this table is logged by database auditing tools
• MCRSPOS database • CCBATCH_AUTH_DETAIL table	Auth Code	Plain Text	Access to this table is logged by database auditing tools
• LOCATION_ACTIVITY database • GUEST_CHECK_LINE_ITEM table	Cardholder name[1] Last 4 digits of account number	Plain Text	Access to this table is logged by database auditing tools Reporting and Analytics report
Guest check files are on the workstation stored in the checks folder under the application root.	Primary Account Number (PAN) depending if manual or swipe entry Cardholder name[1] Expiration Date Auth Code	AES-256 encryption using RSA 2048 bit key pairs	N/A
Offline Transaction Files are stored on the workstation under application root.	Primary Account Number (PAN) depending if manual or swipe entry Cardholder name1 Expiration Date Auth Code	AES-256 encryption using RSA 2048 bit key pairs	Binary files are deleted after application comes back online and checks are transferred o application server.

[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.*

Data Store	Cardholder Data Elements stored	How the Data Store is secured	How is access to Data Store logged
• MCRSPOS database • POS_JOURNAL_LOG table	Cardholder name1 Last 4 digits of account number	Plain Text	Access to this table is logged by database auditing tools
• LOCATION_ACTIVITY database • POS_JOURNAL_LOG table	Cardholder name1 Last 4 digits of account number	Plain Text	Access to this table is logged by database auditing tools Reporting and Analytics report

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 3.2 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 Simphony First Edition 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.

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 Simphony First Edition 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 (PA-DSS 1.1.4)
- Handling of Sensitive Authentication Data (PA-DSS 1.1.5)
- Secure Deletion of Cardholder Data (PA-DSS 2.1)
- All PAN is Masked by Default (PA-DSS 2.2)
- Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5)

- Removal of Historical Cryptographic Material (PA-DSS 2.6)
- Set up Strong Access Controls (PA-DSS 3.1 and 3.2)
- Properly Train and Monitor Admin Personnel
- Log Settings must be Compliant (PA-DSS 4.1.b and 4.4.b)

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 data.

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

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

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

However, if for any reason you should do so, the following guidelines must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect SAD only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt such data while stored.
- Securely delete such data immediately after use.

Secure Deletion of Cardholder Data (PA-DSS 2.1)

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

- A customer defined retention period must be defined with a business justification
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted

Here are the locations of the cardholder data that you must securely delete:

- SECURE_DETAIL

- QUE_CHECKS
- QUE_CHECKS_HIST
- QUE_CHECKS_INPROC
- QUE_CHECKS_RETRY
- CCBATCH_DETAIL
- CCBATCH_AUTH_DETAIL
- WS_OTF
- Cardholder Data must be securely deleted within the transaction database. To securely delete Cardholder Data you must perform the steps as outlined in the Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4).
- 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.

The PAN data is immediately encrypted with the Data Encryption key once successful authorization is acquired. Simphony First Edition automatically securely deletes Cardholder Data by overwriting memory with 0's. No further access to PAN data occurs until the payment object is used at the Hosting Center during the credit card settlement process.

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 on page B-1 of Appendix B.

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.

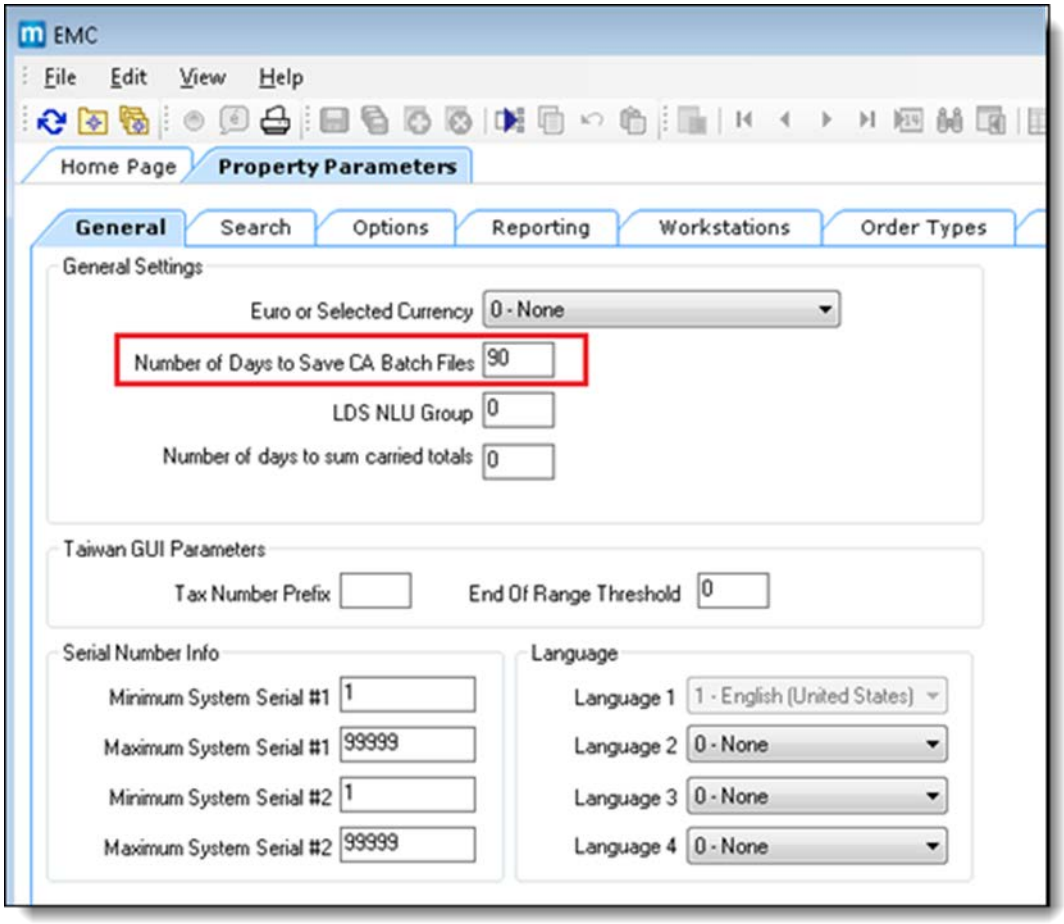
First, configure the system from the Enterprise level. To begin:

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)

Simphony First Edition 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 version 3.2. Simphony First Edition 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).

The payment application displays PAN in the following locations:

- Operator Display
- Guest check receipt – masks all but the last four digits of the PAN. No expiration date.
- CA voucher receipt – masks all but the last four digits of the PAN. No expiration date.
- EMC CC Batch Module – masks all but the last four digits of the PAN. Masks the expiration date.
- R&A Check Detail Report – masks all but the last four digits of the PAN. Masks the expiration date.
- R&A CC Batch Detail Report – masks all but the last four digits of the PAN. Masks the expiration date.
- R&A Audit and Analysis Journal Report – masks all but the last four digits of the PAN. No expiration date.

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 version 3.2.

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

- You must restrict access to encryption keys to the fewest number of custodians necessary
- You must store encryption keys securely in the fewest possible locations and forms
- A sample Key Custodian form has been provided on page C-1 of Appendix C 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 Simphony First Edition key rotation process.

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

- Performing the key rotation as outlined in the *Simphony First Edition Security Guide* 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

Simphony First Edition 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.

Simphony First Edition uses credit card masking and AES-256 encryption to ensure credit card data is stored in a manner compliant with the PCI Data Security Standard.

Oracle Food & Beverage recommends that customers or resellers\integrators rotate the keys every 180 days. The *Simphony First Edition Security Guide* 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)

Simphony First Edition has the following versions that previously encrypted cardholder data:

- Simphony First Edition version 1.5 – 1.5.500
- Simphony First Edition version 1.6 – 1.6.1000
- Simphony First Edition version 1.7 – 1.7.1000
- Simphony First Edition version 1.8

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 First Edition Security Guide* document (in the Appendix) states that Simphony First Edition 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 the *Simphony First Edition Security Guide*.

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® MICROS 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)

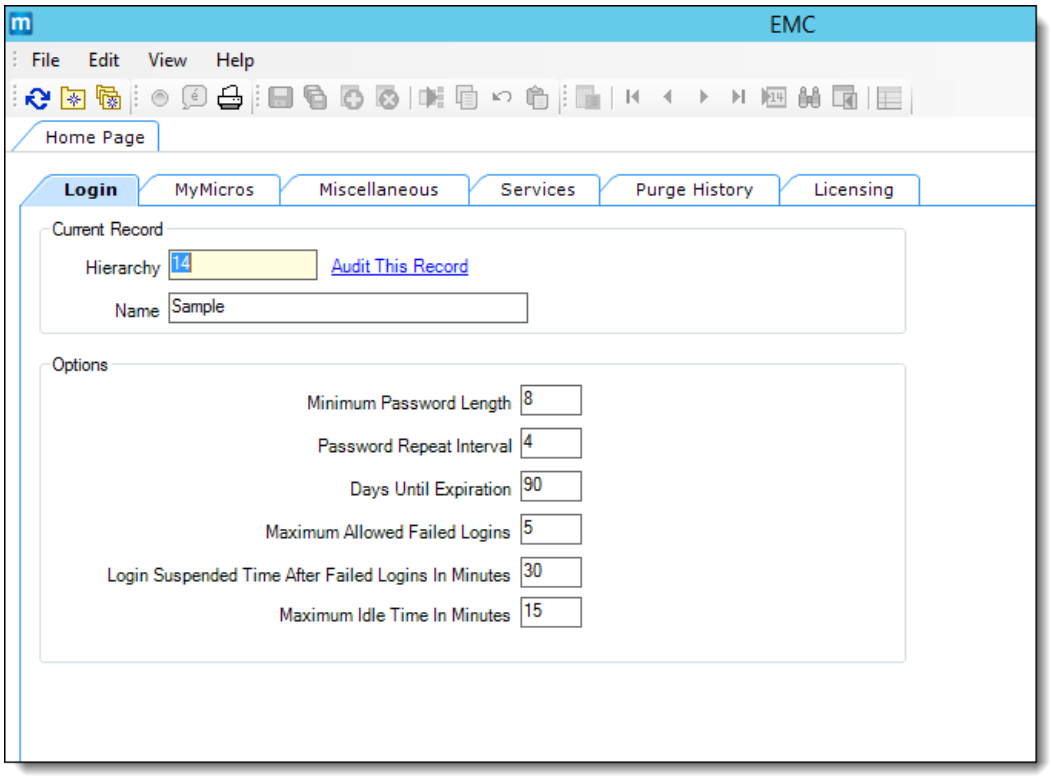
How to create a PCI compliant password in the Simphony Enterprise Management Console (EMC)

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 Simphony First Edition application, always assign unique usernames and complex passwords to each account. Oracle Food & Beverage mandates applying these guidelines to not only Simphony passwords but to Microsoft Windows operating system passwords as well. Furthermore, Oracle Food & Beverage 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.

Configuring a Strong Password Policy

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, 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.

Changing User Passwords

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

User Initiated Password Change

1. From the EMC, click **Edit** on the toolbar and select **Change Password**.
2. Enter the Current Password, New Password, and then Confirm New Password.
3. Click **Accept**.

Administrator Initiated Password Change

Make sure you have sufficient privileges for changing passwords (Privileges are managed in EMC, Roles, and the EMC Modules tab).

1. From the EMC, navigate to Employee Maintenance.
2. Select an employee whose password needs to be changed.
3. Select the employee's record.
4. Select the **Password** button under the EMC Login section.

5. Enter the New Password, and Confirm New Password.
6. Click **Accept**.

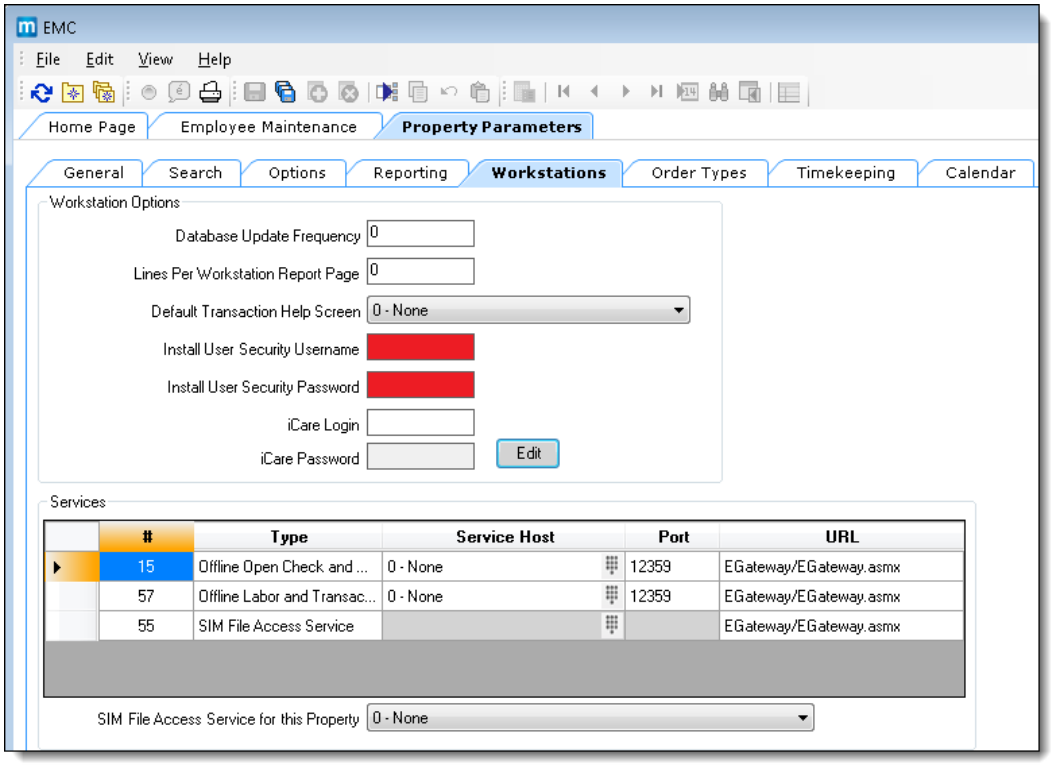
Property Password Maintenance

Change your Simphony First Edition Property's Install Username Password.

Configure Workstation Installer Password

Make sure you have sufficient privileges for changing passwords. Privileges are managed in EMC, Roles, and the EMC Modules tab.

1. From the EMC, navigate to Property Parameters, and select the **Workstations** tab.
2. Enter the Install User Security Username and Install User Security Password which is used to install and authenticate all workstations that Simphony First Edition uses to access the enterprise for the specified property.



3. After entering the username and password, click **Save**.

Repeat these steps for all of the properties in the Enterprise.

The *Simphony First Edition Security Guide* contains additional details about securely configuring user accounts and user privileges.

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

- Simphony First Edition
- 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. 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: Simphony First Edition 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 First Edition in any way results in non-compliance with PCI DSS.

4.1.b: Simphony First Edition 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 Simphony First Edition in any way results in non-compliance with PCI DSS.

4.4.b: Simphony First Edition facilitates centralized logging.

Database Logging

Enable the Oracle Audit Trail

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 Language Reference.

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`.

Enable Microsoft SQL Server Auditing

For customers interested in implementing more extensive auditing within Microsoft

SQL Server, see the information on C2 audit tracing for MS SQL Server, by following the link to the Microsoft Developer Network website,

http://msdn.microsoft.com/en-us/library/ms187634(v=SQL.100).aspx

The EMC Audit Trail

In accordance with the PCI Data Security Standard, Oracle Food & Beverage 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 First Edition database Audit Trail utility is automatically enabled by default and requires no initial configuration. For more information about the Audit Trail Utility see the *Simphony First Edition Security Guide.*

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

Oracle MICROS Simphony First Edition 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 *Oracle MICROS Hardware Wireless Networking Best Practices Guide* 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.

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:

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 First Edition Security Guide* contains more information about the encryption key rotation process.

Default SNMP community strings on wireless devices must be changed.

Default passwords/passphrases on access points must be changed.

Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.

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.c)

This chapter provides guidelines for the following services and protocols:

- Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.c)
- PCI-Compliant Remote Access (PA-DSS 10.1)
- PCI-Compliant Delivery of Updates (PA-DSS 7.2.3, 10.2.1.a)
- PCI-Compliant Remote Access (PA-DSS 10.3.2.a)
- Data Transport Encryption (PA-DSS 11.1.b)
- PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)
- Non-Console Administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)
- Network Segmentation
- Maintain an Information Security Program
- Application System Configuration
- Payment Application Initial Setup & Configuration

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

Simphony First Edition utilizes the following protocols when supporting wired or wireless network connections for payment devices:

- SOAP used by XML Web service
- TCP\IP and proprietary protocol
- Transport Layer Security (TLS) 1.2

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

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.) The enabling of the following ports is recommended to keep systems storing cardholder data separate from Internet connection access. Enable Firewall settings accordingly.

Simphony First Edition Enterprise Ports

Service	Port Number	Configurable?
Database Default (Oracle)	1521	Yes
Database Default (Microsoft SQL Server)	1433	Yes
Simphony/EGateway Application server (Oracle/SQL)	8080	Yes
• EMC/Remote EMC • CAL Client • CAL Handler • Classic CAL Service	8080 7301 (UDP) 7301 (UDP) 7301 (UDP)	Yes Yes Yes Yes
Reporting and Analytics (formerly mymicros.net)	80 - Browser 81 - myLabor service	Yes

Simphony First Edition Property Ports

Service	Port Number	Configurable?
SarOps	12359	No
CAL Client	7300, 7301, 7302	Yes
Offline Labor/Check Cache (running on SarOps)	12359	Yes
Offline Labor/Check Cache (stand-alone ServiceHost)	8080	Yes
IP Printing	9100	Yes
IP Printer Listening	9100	No
Banquet Printing	9100	No
KDS Client (Display)	12359 & 5022 (preferred)	No
KDS Controller Service	12359 & 5023 (preferred)	Yes
Interface Service	8080 (Client & external sides)	Yes

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 are most likely be exceptions to this rule.
Other ports: Make sure to check the wrapper.conf for environment-specific mymicros ports using this Simphony First Edition 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. This 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 First Edition 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 First Edition is required to accomplish this.

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

Simphony First Edition 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**

  Beginning on 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 Pre-Release Advisory is published by Oracle. Both the Pre-Release Advisory and the CPU Release Documentation are posted on the Critical Patch Updates and Security Alerts page on Oracle's web site located at:
  `https://www.oracle.com/technetwork/topics/security/alerts-086861.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-256) checksum for the downloaded patch file. You can use a tool like the Microsoft File Checksum Integrity Verifier, or a similar MD5 and SHA-256 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 MICROS Simphony First Edition 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 MICROS Simphony First Edition 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 10.3.2.a)

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

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.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either using TLS 1.2 or internet protocol security (IPSEC); or at the data layer with algorithms such as RSA or AES-256) 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 1.2 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 MICROS Simphony First Edition, these settings are not user configurable.

Communication is secured using RSA 2048. PAN data is immediately encrypted with the Enterprise Server Public key once successful authorization is acquired in the payment application using RSA 2048. 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 Simphony First Edition.

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

Oracle MICROS Simphony First Edition does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

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

Oracle MICROS Simphony First Edition 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 1.2 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.

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 10
- Microsoft Windows 8.1
- Microsoft Windows Embedded POSReady 7
- Microsoft Windows Embedded Compact
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Oracle Enterprise Linux versions 6.x (database servers only)
- Oracle Database 12c
- Oracle Database 11g

- Microsoft SQL Server 2016

Payment Application Initial Setup & Configuration

Stunnel Configuration

When the Simphony First Edition CAPMS driver is used for credit card transaction processing, the credit card payment provider supplies the recommended Stunnel configuration to ensure strong encryption (TLS 1.2 or higher) of transmitted data. The payment provider also ensures the recommended secure ciphers are enabled. The recommended list of ciphers is as follows:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

Additional Resources

- *Oracle MICROS Simphony First Edition 1.8.0 Installation Guide*
- *Simphony First Edition Security Guide*

Appendix A
Data Security

Data Security

Data security is a vital component of the Simphony First Edition Version 1.8.x.x services infrastructure. Critical financial, transactional, and sensitive data is protected as it is routed between the Simphony First Edition workstation and between the credit card 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
- Workstation 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 Simphony First Edition 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 Simphony First Edition to protect both the sensitive data that is stored and transmitted by Simphony First Edition 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 workstations 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 Data Encryption Key Generation

A username and password must be entered prior to being able to use a Simphony First Edition OPS client. In addition to authorizing the client to perform transactions, a RSA 2048-bit strength key pair, called the Encryption 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 the public and private halves of the key pair 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 which includes the new keys in addition to a version number.

The OPS client 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 First Edition Ops client encrypts data which is deemed secure prior to storing it in the client database, e.g. credit card authorization data. The secure data is encrypted using the public half of the Encryption Key which it was issued when the client was authorized. Finally, the encrypted data is stored in 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 Ops client to be transmitted to the credit card service for requests to the processor.

When that time arrives, the OPS client will package together a message which contains the following information:

- The secure data encrypted using a one-time AES-256 key
- The encrypted AES-256 key
- The remaining check data, e.g., header information, menu items, discounts, service charges, etc.

The Ops client will request the public half of the RSA 2048-bit key that is unique to the receiving service. Then, the Ops client will encrypt the message contents with a one-time generated AES-256 key and encrypt the AES-256 key using the public half of the RSA key that was obtained from the receiving service.

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 AES-256 key, and then decrypt the message information with the one-time key. The message contents are then transmitted to the credit card processor across a secure TLS connection to the credit card processor.

Workstation to Enterprise Data Transmission

The workstations transmit check data to the Enterprise. The workstation 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 workstation is received at the Enterprise, the application server will use the private half of the Transmission key pair to decrypt the AES-256 key and use the AES-256 key to decrypt the message contents.

Enterprise Secure Data Storage

If the message received from a Workstation contains secure data within it, the Enterprise application service will go through the following process to break down the message and store it. 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 AES-256 bit encryption and stored in the PASSPHRASE table.

ENCRYPTION KEYS are used to encrypt SECURE DETAIL in the Enterprise database.

When Simphony First Edition 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 AES-256-bit 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 AES-256-bit 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 First Edition 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
Inadvertent Capture of PAN

This appendix provides instructions for addressing the inadvertent capture of PAN

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

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

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

Clear the System PageFile.sys on Shutdown

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

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

Disable System Management of PageFile.sys

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

Disable Error Reporting on the System

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\SOFTWARE\Microsoft\Windows\Windows Error Reporting.
4. Right-click "**Disabled**" and select **Modify**.
5. if "**Disabled**" does not exist, right-click the Windows Error Reporting folder, select New, and select DWORD (32-bit) Value.
6. Set the Value data field to 1 and click OK.

Appendix C

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: _____