Oracle® Hospitality OPERA Property Management

Version: 5.6

SSF Implementation Guide

Document Part Number: F62229-01

Date: August 25, 2022

Guide to this document:

The SSF program provides merchants and other end-users with a level of confidence that the application they are using to process payment card data can facilitate and support a PCI DSS compliant environment. This document is designed to contain a large amount of sensitive information about the security of the application to be reviewed. It should be filled out as detailed as possible to provide Coalfire with the required information needed to carry out the SSA audit.

Table of Contents

Revision Information

Name	Title	Date of Update	Summary of Changes
Oracle Hospitality OPERA Property Management	SSF Implementation Guide	August 25, 2022	Implementation of Coalfire requested changes.

1 Executive Summary

OPERA Property Management 5.6 has been Software Security Framework (SSF) validated, in accordance with SSF Version 1.1. For the SSF assessment, we worked with the following PCI SSC approved Secure Software Assessor :

Coalfire Systems, Inc. 11000 Westmoor Circle, Suite 450, Westminster, CO 80021	Coalfire Systems, Inc. 1633 Westlake Ave N #100 Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Software Security Framework (SSF) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality OPERA Property Management Version 5.6 and higher as a SSF 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 (SSF, PCI DSS, etc):

- Software Security Framework (SSF)
  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

Software Name	OPERA Property Management	**Payment Application Version**	5.6
Payment Application Description	OPERA Property Management is a Windows-based software application used to process payment card payments. The application can accept both card present and card-not-present transactions. OPERA Property Management Version 5.6 does not support PIN-based debit transaction nor does it include the capability to perform chargebacks. For the purpose of settling transactions, the application retains the PAN, expiry date, and cardholder name in an Oracle 19c using AES256 encryption for the data at rest. The application also stores the truncated card number with just the last four digits of the PAN, if needed for reference by the merchant employee. Cardholder data can be either swiped or manually entered into the application. When manually entered, card validation codes are requested. All sensitive authentication data collected during a transaction, including PAN, magnetic track data and card validation codes, CVV2, is stored in VRAM prior to authorization. Subsequent to authorization, data is purged from VRAM. OPERA Property Management Version 5.6 is only sold as a software package with the responsibility of hardware purchase up to the customer. Oracle provides functionality within OPERA Property Management to enter sensitive personal information (including 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 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).		
Typical Role of the Payment Application	OPERA Property Management is a payment application used in hotels for processing credit card transactions and handling authorization and settlement. OPERA Property Management can handle card-present and card-not-present transactions but not debit or other PIN-based transactions. The application consists of a PC-based POS terminal client, an application server, and a database server. The application accepts cardholder data, including PAN, magnetic track and CVV2 codes, directly through the POS terminal client, which passes the cardholder data to the application server, which is used to facilitate the authorization of transactions through communications with the merchant's processor. The database stores cardholder data, including		

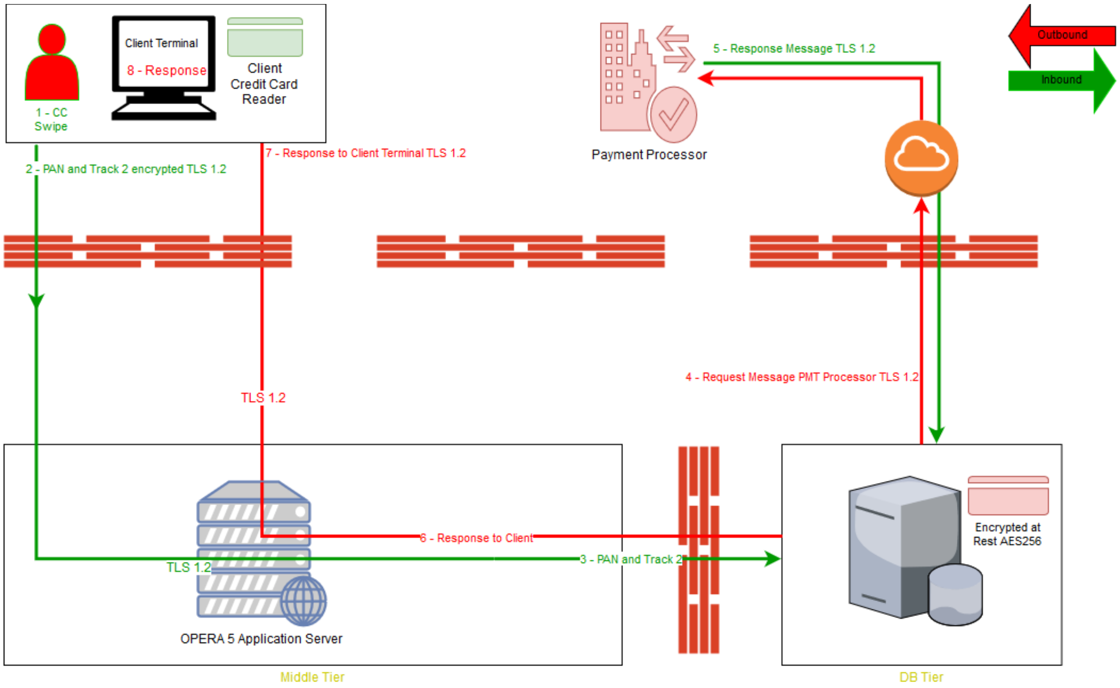
<table>
<tr><td></td><td>the PAN, cardholder name and expiry date only for the purpose of settlement of transactions, using AES256 encryption. The OPERA software resides on both the POS terminal clients and the application server.</td></tr>
<tr><td><b>Target Market for Payment Application (check all that apply)</b></td><td><table>
<tr><td>□</td><td>Retail</td><td>□</td><td>Processors</td><td>□</td><td>Gas/Oil</td></tr>
<tr><td>□</td><td>e-Commerce</td><td>□</td><td colspan="3">Small/medium merchants</td></tr>
<tr><td>☒</td><td colspan="5">Hospitality Industry</td></tr>
</table></td></tr>
<tr><td><b>Stored Cardholder Data</b></td><td>The following is a brief description of files and tables that store cardholder data.</td></tr>
<tr><td><b>Stored Cardholder Data</b></td><td>The following is a brief description of files and tables that store cardholder data.<table>
<tr><th>File or Table Name</th><th>Description of Stored Cardholder Data</th></tr>
<tr><td>name_credit_card</td><td>Full PAN, cardholder name, expiry date</td></tr>
<tr><td>name_credit_card</td><td>Truncated PAN</td></tr>
</table><b>Individual access to cardholder data is logged as follows:</b>
Access to this table is logged by the Oracle 19c database software.</td></tr>
<tr><td><b>Components of the Payment Application</b></td><td>The following are the application-vendor-developed components that comprise the payment application:
OPERA Property Management is designed to be run on Microsoft Windows-based systems. The application is comprised of an application server, a database server running Oracle 19c and PC-based POS terminal clients. All components are meant to be installed within the customer’s corporate network. The application server provides all communication to the processing bank as well as reporting and management functions. The POS terminal client component runs on Microsoft Windows 10/11. The application server runs on Windows Server 2019 and the database server component runs on Windows Server 2019. The application requires the database server to run Oracle 19c on any platform that is supported by Oracle for that version.</td></tr>
<tr><td><b>Required Third Party Payment Application Software</b></td><td>The following are additional third party payment application components required by the payment application:
Not Applicable</td></tr>
</table>

Database Software Supported	The following are database management systems supported by the payment application:
	The application utilizes the Oracle 19c database server. Encrypted cardholder data, including PANs, expiry date, and cardholder name are stored in the database located on the back office server using AES256 encryption.
Other Required Third Party Software	The following are other third party software components required by the payment application:
	Microsoft Internet Explorer 11.0+ 32-bit only JavaSE 8 latest version Oracle JRE Microsoft Edge (Chromium) with Internet Explorer Compatibility Mode
Operating System(s) Supported	The following are Operating Systems supported or required by the payment application:
	Microsoft Windows x64 (64-bit) 10 11 Windows Server 2019
Payment Application Authentication	Authentication to the POS application is handled separately from the operating system. Authentication credentials are held within the application's database. These credentials are stored in the Oracle Database 19c with DBMS_CRYPTO.SH512. During the authentication process, clear text credentials are not sent over the network. When the POS terminal client initiates a connection to the application server, an HTTPS/TLS 1.2 tunnel is opened between the two. All communication including authentication traffic is encrypted.
Payment Application Encryption	The database server provides back-end storage for application data including cardholder data, the PAN, cardholder name, and expiry date encrypted using AES256 with DBMS_CRYPTO.CHAIN_CBC and DBMS_CRYPTO.PAD_PKCS5. The POS software can be installed on a standard PC with a cash drawer. The application is not designed to be implemented in a web-based environment.
Payment Application Functionality Supported	☐ 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	OPERA Property Management uses the standard Microsoft TCP/IP stack that is included with the Windows Operating system when deployed on an Ethernet network. All communications between the application's components (POS terminal client, application server, and database server) are performed via HTTPS/TLS 1.2 tunnels.
Description of Listing Versioning Methodology	Oracle uses a major.minor.patchset.patchset update scheme for Oracle Hospitality OPERA Property Management versioning. Here is a common example: Oracle Hospitality OPERA Property Management versioning has four levels, Major, Minor, Patchset, and Patchset update: **<Major>.<Minor>.<Patchset>.<Patchset Update**> • **Major** includes substantial modification to the application in both operational functionality and appearance would have an impact on SSF requirements. Ranges from 0-10. • **Minor** identifies the milestone steps towards the next major release and may or may not have an impact on SSF requirements. Ranges from 0-10. • **Patchset** contains moderate enhancements and fixes that will not have an impact on Security or SSF requirements. Ranges from 0 - 999. • **Patchset Update** contains minor enhancements and fixes that will not have an impact on Security or SSF requirements. Ranges from 0- 999. Based on the above versioning methodology the application version being listed with the PCI SSC is 5.6

Credit/Debit Cardholder Dataflow Diagram

OPERA Property Management Services Data Flow Diagram Example


Client Terminal
8 - Response
Client Credit Card Reader
1 - CC Swipe
Payment Processor
5 - Response Message TLS 1.2
Outbound
Inbound
7 - Response to Client Terminal TLS 1.2
2 - PAN and Track 2 encrypted TLS 1.2
4 - Request Message PMT Processor TLS 1.2
TLS 1.2
6 - Response to Client
3 - PAN and Track 2
TLS 1.2
Encrypted at Rest AES256
OPERA 5 Application Server
Middle Tier
DB Tier

1. Client swipes card for card present or enters card data manually for card not present transactions in the browser on the Client Terminal.
2. PAN and Track 2 (if swiped) is sent via HTTPS/TLS1.2 from the Client Terminal browser to the OPERA Application Server.
3. The OPERA Application Server sends this data to the OPERA Database Server and stored encrypted with AES256.
4. The OPERA Database formats the data into a request message and sends the transaction to the Payment Processor.
5. The Processor responds with the approval or decline of the transaction. The PAN and Expiration Date are stored encrypted for any future use related to the original transaction.
6. The OPERA Database sends the response to the OPERA Application Server.
7. The OPERA Application Server directs the response to the correct Client Terminal.
8. The response is displayed to the user to action if needed or to complete the business transaction.

Differences between PCI Compliance and SSF Validation

As the software and payment application developer, our responsibility is to be “SSF validated”. We have performed an assessment and payment application validation review with our independent assessment firm to ensure that our platform conforms to industry best practices when handling, managing, and storing payment- related information.

SSF is the standard against which the Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE).

Obtaining “PCI Compliance” is the responsibility of you the merchant and your hosting provider, working together, using PCI compliant architecture with proper hardware & software configurations and access control procedures.

The SSF Validation is intended to ensure that OPERA Property Management will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

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

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

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

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

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

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

Remove Historical Sensitive Authentication Data

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.

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

OPERA Version 5.6 does not store historical credit card data.

To stay in compliance with the Payment Card Industries – Security Standards Council requirements, when upgrading from a version of OPERA previous to Version 4.0, turn the CC_TRACK2 parameter off in the previous version. This deletes the Track 2 data from the OPERA database. To turn off the parameter in OPERA Version 3.0, select Setup, then Application Settings, and set the IFC Group Application Parameter to No, as shown below.

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

Windows:

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

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

UNIX

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

Shred is included with many distributions of Linux.

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

Handling of Sensitive Authentication Data

OPERA Property Management does not have a debugging mode that could write PAN to debugging logs. The support Team never collects SAD for troubleshooting or any other purpose.

Oracle provides functionality within OPERA Property Management to enter sensitive information such as 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 at rest. Entering this sensitive personal information in any other field (for example, in a Notes or Comments field), does not provide it with these heightened security controls and is not consistent with the requirements for protecting cardholder data as detailed in the Payment Card Industry Data Security Standards (PCI DSS).

Secure Deletion of Cardholder Data

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.
- The default value for the retention period is 180 days.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- Here are the locations of the cardholder data you must securely delete: name_credit_card (Full PAN, cardholder name, expiry date) name_credit_card (Truncated PAN).
- Cardholder Data must be securely deleted within the payment applications and databases. Oracle recommends activating the GENERAL > PURGE UNNECESSARY CREDIT CARDS application setting and entering the number of days to use to determine which credit cards are eligible for removal from the database, provided the credit card is not attached to any other current or future reservations in any property (in multi-property environments). Actual removal is handled by the Purge Credit Cards procedure, which is included in the OPERA Data Purge Routine, and is implemented at the next scheduled run of that routine. Here is how this setting affects credit card information removal. The procedure executes each time the OPERA Data Purge Routine is scheduled. The procedure refers to the Days to Remove Unnecessary Credit Cards setting only to determine all the valid credit card information that is older than that many days.
- Days entered are the days after the departure date of the reservation that was settled by credit card. For example, if Days is set to 5, and the reservation departure date is April 7, the credit card information is eligible to be removed on April 12 (regardless of whether the reservation was cancelled or was no show).
- Days entered are the days after the folio close date (when the CASHIERING OPEN FOLIO application parameter is set to Y) if payment was made by credit card and the reservation is checked out with open folio. For example, if Days is set to 5, and the guest checks out on April 7 with open folio, if the folio is closed on April 11, the credit card information is eligible to be removed on April 16.
- Days entered are the days after reconciliation if the reservation is checked out to a credit card payment method having an AR account attached. For example, if Days is set to 5,

and a reservation checks out paying by credit card, an AR invoice is created in the associated AR account. If this AR invoice is reconciled on May 12, the credit card information is eligible to be removed on May 17 provided this reconciled AR invoice has already been purged. If the invoice is not purged even after reconciliation, the credit card information will NOT be removed.

- Days entered are the days after the credit card information has been added to the profile (available when the PROFILES > PROFILE CREDIT CARD application function is set to Y), provided the credit card has not been attached to any current or future reservations. For example, if Days is set to 5, and the credit card information is attached to a profile on April 7, the credit card information is eligible to be removed on April 12.
- Credit card information will NOT be removed in case there is a pending batch/offline settlement for the credit card.
- For all users, credit card information is only available in truncated format (e.g., XXXXXXXXXXXX4317, expiration date XX/XX) once it has been removed from the database. (After the purge routine runs, all that actually remains of the credit card number in the OPERA database is the last four digits; all other credit card information, including the expiration date, is entirely removed.) The truncated format information is displayed, as required, in screens and in response to requests for reports and historical information.
- All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in Appendix A.

All PAN is Masked by Default

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

- All printed receipts.
- All generated card reports in the reports menu; these include the following reports:
- AR Credit Invoice (arcrdlist)
- AR Credit Card Transfer (arcrtransfer)
- AR Ledger (arledger)
- Membership Pre-Check In (arrprecheckinmem)
- Check Report (check_rep)
- Credit Card History (creditcard_history)
- Credit Card Rebates (creditcard_rebates)
- Credit Card Authorization History (cc_auth_history)
- Journal by Cashier and Article Code (finjrnl_articles)
- Journal by Foreign Currency (finjrnlbyforcurr)
- Financial Transactions by Tax Type (finjrnlbytax)
- Journal By Cashier and Transaction Code (finjrnlbytrans)
- Financial Transactions with Generates (finjrnlbytrans2)
- Cashier Audit (finpayments)
- Credit Limit Report- All Payment Methods (gi_authlimit)
- Rate Variance (giratevariance)

- Group Rooming List (grprmlist)
- Night Audit Credit Card Authorization (nacc_authorization)
- No Shows of the Day (nanoshow)
- Paid Outs (napaidout)
- No Show Extended Reservations (noshow_ext)
- Arrivals Detailed (res_detail).

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

Cardholder Data Encryption & Key Management

OPERA Property Management store cardholder data always encrypted using AES256 and does not have the ability to output PAN data in clear text for storage.

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

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

Removal of Historical Cryptographic Material

- Removal of historical Keys is not needed.

Set up Strong Access Controls

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.

Do not share User IDs or Passwords.

The following roles and default accounts within the application have administrative access.

- Supervisor
- Member of OPERA Supervisor Role

All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts). To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts). (PCI DSS 2.1)
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)
3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1)
4. The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2)
   a. Something you know, such as a password or passphrase
   b. Something you have, such as a token device or smart card
   c. Something you are, such as a biometric
5. The payment application must not require or use any group, shared, or generic accounts and passwords. (PCI DSS 8.5)
6. The payment application requires passwords to be at least 7 characters and include both numeric and alphabetic characters. (PCI DSS 8.2.3)
7. The payment application requires passwords to be changed at least every 90 days. (PCI DSS 8.2.4)
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)
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)
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)
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)

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

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

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

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.

If the historical Cardholder data is no longer needed, the following must be completed to ensure PCI Compliance:

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

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

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

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

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

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

These screens include the Reservation screen, the Payment screen, the Profile screen, the Group Rooming List, and others.

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

10.2.1 All individual user accesses to cardholder data from the application

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

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

10.2.4 Invalid logical access attempts

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

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

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

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

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

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

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

3 PCI-Compliant Wireless Settings

OPERA Property Management does support wireless technologies and the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1, and 4.1.1:

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

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. Default SNMP community strings on wireless devices must be changed.
3. Default passwords/passphrases on access points must be changed.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

4.1. 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

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

- TLS1.2 or higher PROTOCOLS UTILIZED
- SFTP
- HTTPS
- IPSec
- Opera utilizes Port 443 for the forms application

Oracle recommends that all sensitive information that is transmitted over the Internet be secured using a form of encryption such as TLS 1.2 Protocols.

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

Oracle strongly suggests that when using our web based credit card interface, it is set up to use TLS 1.2 Protocol communication. To configure this, do the following: Select Configuration, then Setup, then Property Interfaces, and then select Interface Configuration and edit the active EFT Interface. On this form you will see a section to configure the URL that you are to connect to. Be sure that this URL starts with HTTPS. This will ensure a secure TLS 1.2 Protocol connection is made to the vendor prior to transmitting credit card data.

Never Store Cardholder Data on Internet-Accessible Systems

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access

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

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

PCI-Compliant Delivery of Updates

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

PCI DSS 1

Install and maintain a firewall configuration to protect cardholder data.

PCI DSS 12.3.9

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

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

Once we identify a relevant vulnerability, we work to develop and test a patch that helps protect OPERA Property Management against the specific new vulnerability. We attempt to publish a patch within 10 days of the identification of the vulnerability. We then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

We deliver software and/or updates via download access to customer networks. These are made available on the Oracle website < https://support.oracle.com > for download.

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

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

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

Critical Patch Updates (CPU) are delivered quarterly and information is available on the Oracle website: https://www.oracle.com/security-alerts/.

All Oracle install media is digitally signed.

PCI-Compliant Remote Access

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:

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

OPERA Property Management on-premise installations must not be directly accessible through the internet and any Administration must be done within the Customer network.

Data Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with TLS or IPSEC; or at the data layer with algorithms such as RSA or AES256) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

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

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

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

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with OPERA Property Management.

PCI-Compliant Use of End User Messaging Technologies

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

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

Non-Console Administration and Multi-Factor Authentication

OPERA Property Management server does not allow non-console administration.

Network Segmentation

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

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with OPERA Property Management.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

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

Microsoft Windows x64 (64-bit)	10 11 Windows Server 2019

Payment Application Initial Setup & Configuration

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

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

- Property Interface > General tab > CC Vault Function
- Property Interface > Custom Data tab > VAULT_ID
- Property Interface > Custom Data tab > VAULT_MAX_CC_PROCESSED
- Property Interface > Custom Data tab > VAULT_CERT_CHAIN_CODE
- Property Interface > General Tab > URL/Token URL
- Property Interface > Custom Data tab > WALLET_PASSWORD
- Property Interface > Custom Data tab > HTTP_USERNAME
- Property Interface > Custom Data tab > HTTP_PASSWORD

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

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

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

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

A. Save the vendor provided .crt and .p12 on the workstation.

B. Run **MMC** and import the certificate using the following steps.

   1. Go to **File > Add or Remove Snap-ins**.
   2. Select **Certificates** under the Available snap-ins section and add it to the selected **snap-ins** section.
   3. On the Certificates snap-ins screen, select **Computer Account** and then click **Next**.
   4. Keep the option **Local computer** and click **Finish**.
   5. Click **OK** to go back to the main MMC window.
   6. Right-click on a folder under the Certificates folder and select **All Tasks** followed by **Import.**

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

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

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

A successful response is similar to this:

```
Microsoft (R) WinHTTP Certificate Configuration Tool Copyright
(C) Microsoft Corporation 2001.
```

An unsuccessful response may be similar to this:

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

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

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

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

- Installing the Payment Application – the needed DLLs and jar files are automatically downloaded with the OPERA installation. With the above application settings active and certificates installed, the Payment App will be available from the icon on the OPERA forms.
- Defining the Payment Gateway - use TLS1.2 or higher for communication between OPERA and the EFT system. The vendor provided .p12 is used as the Server side certificate and imported to the Oracle Wallets folder on the OPERA database server.
- Obtaining and Install the 128 bit TLS 1.2 Protocol Certificate.
- Conducting Test Transactions - can be completed only if Vendor supports test card data.

- Special Instructions for Upgrades – existing card numbers in the OPERA database can be converted to tokens from the EFT system in a process initiated through OPERA Utilities.
- Resetting Administrator Passwords - OPERA User Passwords have mandatory expiry every 30 days.
- Performing Maintenance - recommend setup purge of historical data.
- Updating your Encryption Key on a Periodic basis - recommend setup purge of historical data and execute the Sensitive Information Encryption Key Utility. This is not needed when Vault is active.

SSF required File Integrity Monitoring (FIM)

File Integrity Monitoring (FIM) can be provided by 3rd party products through agents that are installed on Windows servers.

Customers will need to configure the FIM solution of their choice according to the 3rd party configuration and installation manual.

Any FIM solution used must define the frequency for which the integrity values should be checked. The minimum value for integrity checking should be set to at least every 36 hours.

A Watchlist is a combination of file names and directories which has been defined to be monitored along with the type of event which needs to be monitored. Attributes which can be monitored on the files are:

- File Create
- File Write
- File Delete
- File Rename
- File Permission Change

Files that should be monitored:

Component	File	Location	Functionality	Description
OPERA folder (\Micros\Opera)	opera.cfg	\Micros\Opera\operaias.	Config file with home locations, client home location, JDK, etc.	Created / updated only by installation
	opera.conf		OHS config file (included in httpd.conf)	included in httpd.conf of OperaOHSDomain
	opera_wl.conf		OHS/Weblogic context root configuration	Updated when new applications are deployed