Oracle® Hospitality OPERA Cloud Services

PA-DSS 3.1 Implementation Guide
Release 1.20
Part Number: E69080-01

February 2016

Contents

1 Preface

This document describes the steps that you must follow in order for your Oracle Hospitality OPERA Cloud Service (OPERA Cloud) installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.1 dated May 2015). You can download the PCI PA-DSS 3.1 Requirements and Security Assessment Procedures from the PCI SSC Document Library.

Oracle Hospitality instructs and advises its customers to deploy Oracle Hospitality applications in a manner that adheres to the PCI Data Security Standard (v3.1). Subsequent to this, you should follow the best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various benchmarks, in order to enhance system logging, reduce the chance of intrusion, increase the ability to detect intrusion, and other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling infrequently-used or frequently vulnerable networking protocols, and implementing certificate-based protocols for access to servers by users and vendors.

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

Revision History

Date	Description of Change
December 2015	• Initial publication.
January 2016	• Revised version numbering, revised product naming.

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

2 Executive Summary

OPERA Cloud 1.20 has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.1. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450,
Westminster, CO 80021

Coalfire Systems, Inc.
1633 Westlake Ave N #100
Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality OPERA Cloud 1.20 as a PA-DSS validated application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

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

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP)
  http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

Payment Application Summary

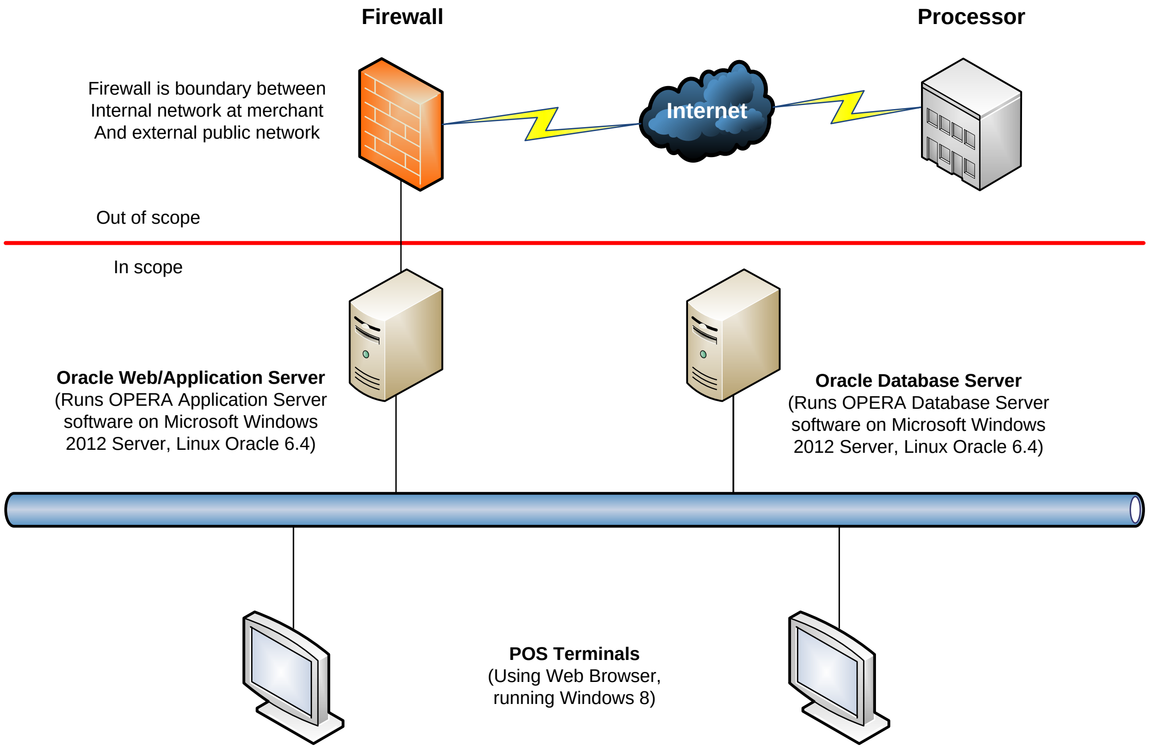
Payment Application Name	OPERA Cloud	**Payment Application Version**	1.20
Payment Application Description	OPERA Cloud is a Windows-based software application used to process payment card payments. The application can accept both card present and card-not-present transactions. OPERA Cloud Version 1.20 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 11g database, 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 Cloud 1.20 is only sold as a software package with the responsibility of hardware purchase up to the customer. **Oracle provides functionality within OPERA Cloud 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 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 Cloud 1.20 is a payment application used in hotels for processing credit card transactions and handling authorization and settlement. OPERA Cloud 1.20 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 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.		

<table>
<tr><td rowspan="4"><b>Target Market for Payment Application (check all that apply)</b></td><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">Others (please specify): Hospitality Industry</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="5"><b>Stored Cardholder Data</b></td><td colspan="6">The following is a brief description of files and tables that store cardholder data.</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="3">File or Table Name</td><td colspan="3">Description of Stored Cardholder Data</td></tr>
<tr><td colspan="3">name_credit_card</td><td colspan="3">Full PAN, cardholder name, expiry date</td></tr>
<tr><td colspan="6"><b>Individual access to cardholder data is logged as follows:</b>
Access to this table is logged by the Oracle 11g database software.</td></tr>
<tr><td rowspan="2"><b>Components of the Payment Application</b></td><td colspan="6">The following are the application-vendor-developed components which comprise the payment application:</td></tr>
<tr><td colspan="6">OPERA Cloud is a web based software that is designed to be browser agnostic.
There are three main components of the payment application:
• The Web client component which runs on various publicly available browsers.
• The Weblogic Middleware server typically runs on Windows Server 2012 or Oracle Linux 6.4
• The database server component runs on Windows Server 2012 and Oracle Linux 6.4. The application requires the database server to run Oracle 11g.</td></tr>
<tr><td rowspan="2"><b>Required Third Party Payment Application Software</b></td><td colspan="6">The following are additional third party payment application components required by the payment application:</td></tr>
<tr><td colspan="6">Not Applicable</td></tr>
<tr><td rowspan="2"><b>Supported Database Software</b></td><td colspan="6">The following are database management systems supported by the payment application:</td></tr>
<tr><td colspan="6">The application utilizes the Oracle 11gR2 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.</td></tr>
</table>

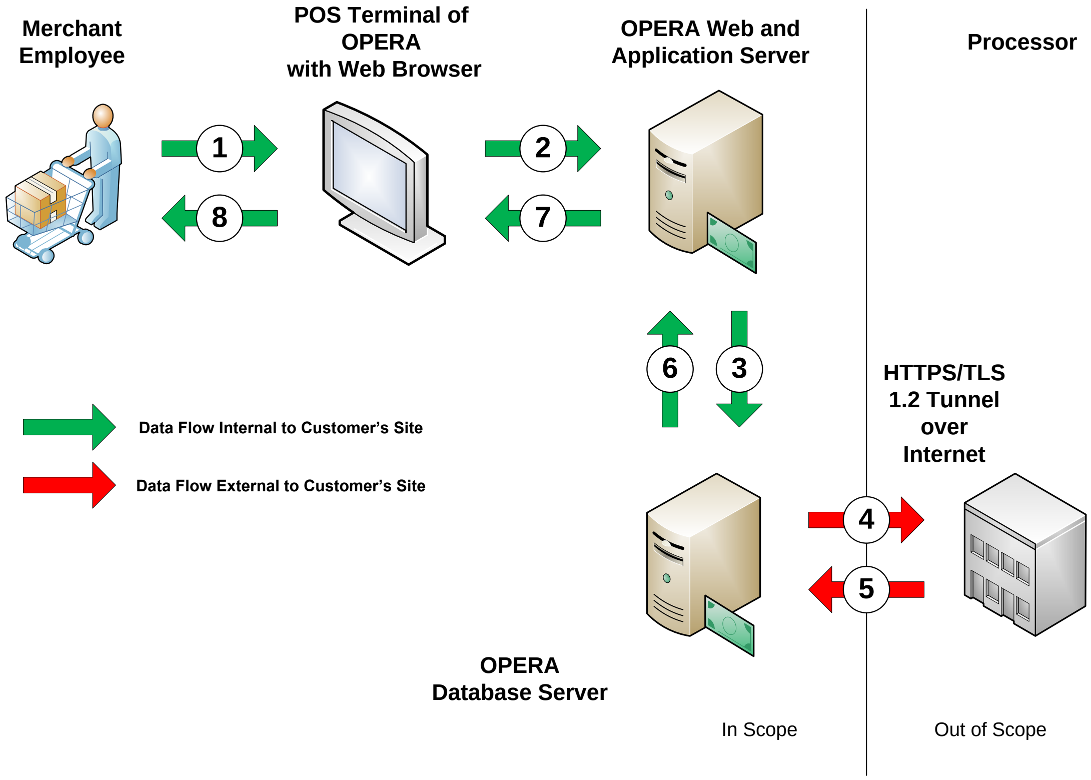
<table>
<tr><td rowspan="2"><b>Other Required Third Party Software</b></td><td>The following are other third party software components required by the payment application:</td></tr>
<tr><td>Not Applicable</td></tr>
<tr><td rowspan="2"><b>Supported Operating System(s)</b></td><td>The following are Operating Systems supported or required by the payment application:</td></tr>
<tr><td>List Operating system(s) and versions/SP’s supported.<table>
<tr><td>Linux x86-64</td><td>Oracle Linux 6.4</td></tr>
<tr><td>Microsoft Windows x64 (64-bit)</td><td>8.1, 7, 2012 R2, 2008 R2</td></tr>
</table></td></tr>
<tr><td><b>Payment Application Authentication</b></td><td>Authentication to the application is handled separately from the operating system. Authentication credentials are stored in a third party Active Directory (AD) service. During the authentication process, clear text credentials are not sent over the network. The systems employs ORACLE’s OAM solution to intercept unauthenticated traffic and references the AD before a SAML token is obtained to allow access. All communication including authentication traffic is done over HTTPS/TLS 1.2.</td></tr>
<tr><td><b>Payment Application Encryption</b></td><td>The database server provides back-end storage for application data including cardholder data, the PAN, cardholder name and expiry date encrypted usingAES256. The POS software can be installed on a standard PC with a web browser.</td></tr>
<tr><td><b>Supported Payment Application Functionality</b></td><td><table>
<tr><td>☐</td><td>Automated Fuel Dispenser</td><td>☐</td><td>POS Kiosk</td><td>☐</td><td>Payment Gateway/ Switch</td></tr>
<tr><td>☐</td><td>Card-Not-Present</td><td>☐</td><td>POS Specialized</td><td>☐</td><td>Payment Middleware</td></tr>
<tr><td>☐</td><td>POS Admin</td><td>☐</td><td>POS Suite/General</td><td>☐</td><td>Payment Module</td></tr>
<tr><td>☒</td><td>POS Face-to-Face/POI</td><td>☐</td><td>Payment Back Office</td><td>☐</td><td>Shopping Card & Store Front</td></tr>
</table></td></tr>
<tr><td><b>Payment Processing Connections</b></td><td>OPERA Cloud 1.20 uses the standard TCP/IP stack that is included with the Windows and Linux operating systems 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.</td></tr>
</table>

Description of Listing Versioning Methodology	Oracle uses a major.development.revision.service pack scheme for OPERA Cloud versioning. Here is a common example: OPERA Cloud versioning has four levels, Major, Development, Revision, and Service Pack: **<Major>.<Development>.<Revision>.<Service Pack>** • **Major** includes substantial modification to the application in both operational functionality and appearance would have an impact on PA-DSS requirements. • **Development** identifies the milestone steps towards the next major release and may or may not have an impact on PA-DSS requirements. • **Revision** contains fixes to moderate defects and may or may not have an impact on PA-DSS requirements. • **Service Pack** contains minor coding enhancements and fixes for minor issues and may or may not have an impact on PA-DSS requirements. Based on the above versioning methodology the application version being listed with the PCI SSC is: 1.20.

Typical Network Implementation


Firewall
Processor
Firewall is boundary between
Internal network at merchant
And external public network
Internet
Out of scope
In scope
Oracle Web/Application Server
(Runs OPERA Application Server
software on Microsoft Windows
2012 Server, Linux Oracle 6.4)
Oracle Database Server
(Runs OPERA Database Server
software on Microsoft Windows
2012 Server, Linux Oracle 6.4)
POS Terminals
(Using Web Browser,
running Windows 8)

Credit/Debit Cardholder Dataflow Diagram


Merchant Employee
POS Terminal of OPERA with Web Browser
OPERA Web and Application Server
Processor
1
8
2
7
6
3
HTTPS/TLS 1.2 Tunnel over Internet
Data Flow Internal to Customer's Site
Data Flow External to Customer's Site
4
5
OPERA Database Server
In Scope
Out of Scope

1. Merchant Employee swipes card data on POS terminal or enters card data manually for card not present transactions into the POS terminal.
2. PAN and Track 2 (if swiped) encrypted data are sent from the POS Terminal to the OPERA Application Server.
3. The OPERA Application Server sends this data to the OPERA Database Server.
4. The OPERA Database formats the data into a request message and sends the transaction to the Processor.
5. The Processor responds with the approval or decline of the transaction.
6. The OPERA Database sends the response to the OPERA Application Server.
7. The OPERA Application Server directs the response to the correct terminal.
8. The response is displayed to the user to action if needed or to complete the business transaction.

Difference between PCI Compliance and PA-DSS Validation

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

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

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

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

PCI Compliance is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE). It is the responsibility of you, as the merchant, and your hosting provider to work together to use PCI compliant architecture with proper hardware & software configurations and access control procedures.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

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

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

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

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

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

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

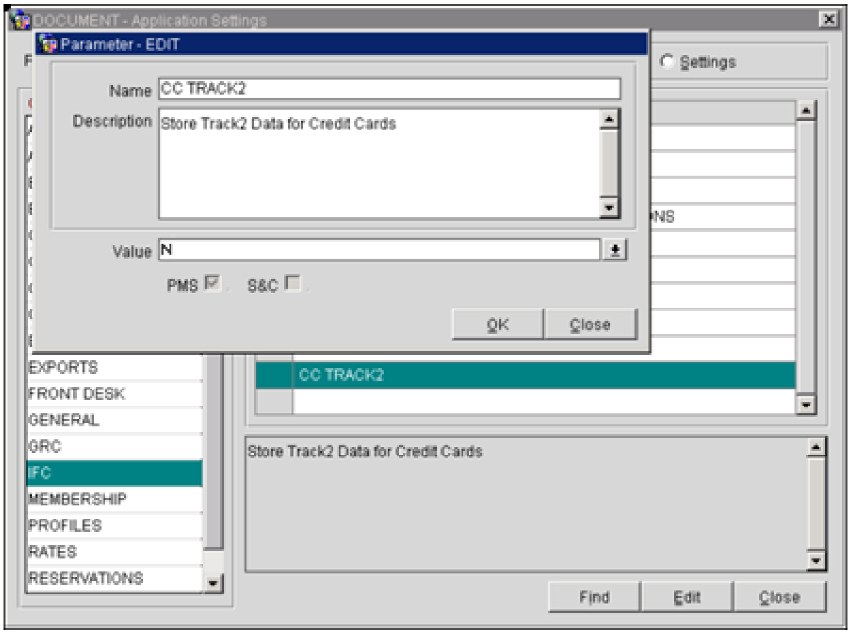
The following previous versions of Oracle Hospitality OPERA 5 stored Sensitive Authentication Data (SAD) including Track 2 data:

- OPERA Version 3
- OPERA Version 2
- Below OPERA Version 2

Historical SAD stored by previous versions of Oracle Hospitality OPERA 5 must be securely deleted and removal is absolutely necessary for PCI DSS compliance. Oracle Hospitality provides a secure deletion tool which includes capabilities to securely delete historical SAD as follows:

After the release of OPERA Version 4, no historical credit card data is stored. But should an upgrade from a version previous to 4 be required, OPERA offers a solution to deleting any sensitive 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, the CC_TRACK2 parameter must first be turned off in the previous version. This will delete the Track 2 data from the OPERA database. To turn off the parameter in OPERA Version 3.0, select **Setup>Application Settings**, and set the **IFC Group Application Parameter** to **N**, as shown below:



Name: CC TRACK2

Description: Store Track2 Data for Credit Cards

Value: N

PMS ☑ S&C □

Store Track2 Data for Credit Cards

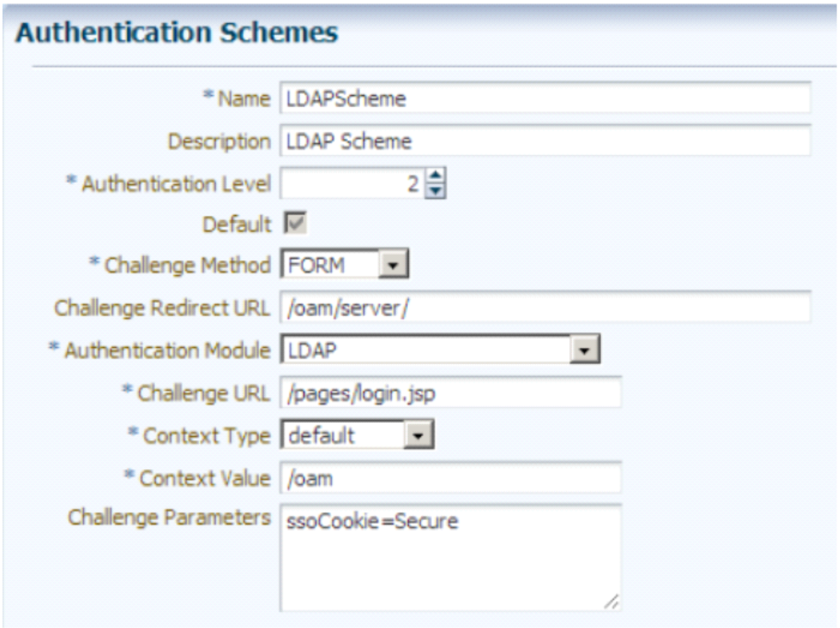
OPERA Cloud, like its OPERA Version 5 predecessor, does not store SAD and is compliant as long as the above condition is ruled out for upgrading clients.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

OPERA Cloud stores Sensitive Authentication Data (SAD) for troubleshooting purposes only and only during the time we are supporting a customer issue. The following guidelines are 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.

For troubleshooting purposes of the Credit Card Vault Conversion Utility, only the records exchanged during the conversion are logged to the table VAULT_CONVERSION_LOG. It is best to run a query in OPERA SQL for the table and then conduct an Export to easily search/view the data (credit card numbers are always masked).



Authentication Schemes

* Name	LDAPScheme
Description	LDAP Scheme
* Authentication Level	2
Default	☑
* Challenge Method	FORM
Challenge Redirect URL	/oam/server/
* Authentication Module	LDAP
* Challenge URL	/pages/login.jsp
* Context Type	default
* Context Value	/oam
Challenge Parameters	ssoCookie=Secure

We strongly recommend that you do not store SAD for any reason. However, if you should do so, the preceding guidelines must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data).

Secure Deletion of Cardholder Data (PA-DSS 2.1)

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

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- Here are the locations of the cardholder data you must securely delete:
  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 (PA-DSS 2.2)

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

- Billing
- Payment Instruction
- Look To Book
- Folio Settlement
- Deposit Payment
- Reservation screen

- Rooming List screen
- Journal screen
- Cashier Reports
- AR Payment screen
- AR Posting History screen
- AR Research screen

OPERA Cloud does not have the ability to display full PAN for any reason and therefore there are no configuration details to be provided as required for PA-DSS v3.1.

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

OPERA Cloud 1.20 does store cardholder data and 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.

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.

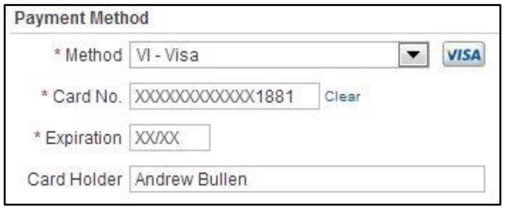
- Generation of strong cryptographic keys.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.
- Retire or replace keys when the integrity of the key has been weakened and/or when known or suspected 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.

Oracle uses credit card masking and AES256 encryption to store the personal account number (PAN), account name, expiration date and ensure credit card data is stored in a manner compliant with the PCI Data Standard.
The OPERA Credit Card Vault functionality automatically encrypts and transports this data to the Vault provider dynamically and eliminates the need to store any actual credit card data in the application.

> **Note:** The Credit Card Vault functionality can only be activated by the IFC>Credit Card Vault application function that is hidden and is a GLOBAL function. If activated in a multi-property environment for one property, then it will be active for all the properties in the environment. Please contact your regional office to get this application function activated and for more details.

To eliminate the storage of credit card numbers in OPERA, Unique IDs (encrypted credit card keys) will be used to replace any credit card numbers; thereafter, these unique IDs will be used for any of the guest's transactions at the property. This Unique ID can be attached to the guest's profile, just as the credit card could be, and will be used for any future stays or transactions that they have.

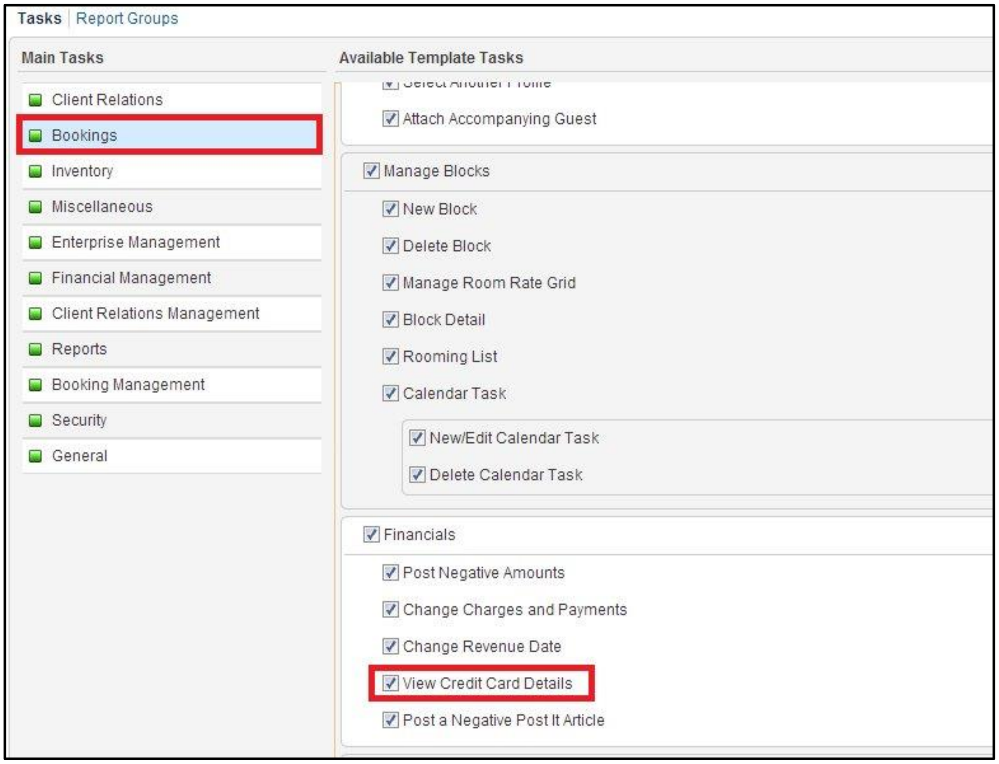
When making a payment in OPERA Cloud, all credit card numbers are masked except for the last 4 digits of the number for reference purposes only.



Payment Method

* Method	VI - Visa
* Card No.	XXXXXXXXXXXX1881
* Expiration	XX/XX
Card Holder	Andrew Bullen

OPERA Cloud masks credit card data natively and only allows the users that have been granted the appropriate View Credit Card Details task to view the details.



☑ Select Another Profile
☑ Attach Accompanying Guest
☑ Manage Blocks
☑ New Block
☑ Delete Block
☑ Manage Room Rate Grid
☑ Block Detail
☑ Rooming List
☑ Calendar Task
☑ New/Edit Calendar Task
☑ Delete Calendar Task
☑ Financials
☑ Post Negative Amounts
☑ Change Charges and Payments
☑ Change Revenue Date
☑ View Credit Card Details
☑ Post a Negative Post It Article

Removal of Historical Cryptographic Material (PA-DSS 2.6)

OPERA Cloud has the following versions that previously encrypted cardholder data:

- OPERA 1.18
- OPERA 1.16
- OPERA 1.14
- OPERA 1.12

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

Note: The following processes should only be used if the Vault functionality is inactive within OPERA and:

1. The Vendor supports it
2. The Vault Conversion tool is configured correctly.

- 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.
- You must manually re-encrypt all historical cardholder data by selecting Utilities > 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: **Reservations > Credit Card Information Edit** and **Utilities > Change Encrypt Key**.
- Previous historical credit card data (no longer needed) must be securely deleted within the payment applications and databases by setting the GENERAL > PURGE UNNECESSARY CREDIT CARDS application setting that runs with the OPERA Scheduler.

Set up Strong Access Controls (PA-DSS 3.1 and 3.2)

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

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

1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
2. The payment application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after the installation (this applies to all accounts, including user accounts, application and service accounts, and accounts used by Oracle Hospitality for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
5. The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)
6. The payment application requires passwords must to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
10. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
11. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

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 Cloud, as tested in our PA-DSS validation, meets, or exceeds these requirements for the following additional required applications or databases.

> **Note**: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to systems with cardholder data, and for access controlled by the application.

The requirements apply to the payment application and all associated tools used to view or access cardholder data.

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

Properly Train and Monitor Admin Personnel

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

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

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

4.1.b: OPERA Cloud 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 OPERA Cloud 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 thus would require logging of user access and activity. Oracle strongly recommends logging of activity on the database server.

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 Cloud in any way will result in non-compliance with PCI DSS.

4.4.b: OPERA Cloud facilitates centralized logging.

The OPERA User Activity Log records a "history" of user activity in the OPERA database and is accessed via Miscellaneous>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 via Cashiering>Credit Cards>Settlement option, or when End of Day attempts to perform the settlement of temporarily stored offline settlements.

> **Note:** The user activity log records each time any user who is granted the RESERVATIONS > CREDIT CARD INFORMATION VIEW permission accesses an OPERA screen to view credit card information (i.e., credit card numbers and expiration dates). 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.

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

OPERA Cloud does support wireless technologies within the payment application 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:

PCI DSS 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.

PCI DSS 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.

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

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

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

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

- SSL PROTOCOL
- SFTP
- HTTPS
- IPSec

Oracle recommends that all sensitive information that is transmitted over the Internet be secured using a form of encryption such as SSL Protocol; this includes all wireless transmissions, email and use of services such as Telnet and FTP.

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). Please refer to IPSecConfig.pdf for configuration.

Oracle strongly suggests that when using our web based credit card interface, it is set up to use SSL Protocol communication. To configure this, do the following. Select **Configuration>Setup>Property Interfaces>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 SSL Protocol connection is made to the vendor prior to transmitting credit card data.

Technical Information Disclosure in Header

HTTPD.CONF has ServerToken setting set to PROD. With this set to PROD Headers will show server information. Below script can be used to disable this, additional settings provided below will fix other Apache vulnerabilities and also steps to disable usage of port 80.

Open a CMD prompt as Admin

```
echo Header unset Range
>>D:\ORA\operainstance\config\OHS\ohs1\HTTPD.CONF

echo FileETag -INode
>>D:\ORA\operainstance\config\OHS\ohs1\HTTPD.CONF

d:\micros\opera\tools\SnR /D=D:\ORA\operainstance\config\OHS\ohs1
/F=httpd.conf /A="ServerTokens Prod" /R="ServerTokens None" /S /I

d:\micros\opera\tools\SnR /D=D:\ORA\operainstance\config\OHS\ohs1
/F=httpd.conf /A="Listen 80" /R="Listen 127.0.0.1:7080" /S /I

del d:\temp\sslinfo.txt
```

```
echo SSLSessionCacheTimeout 300>d:\temp\sslinfo.txt

echo SSLProtocol -ALL +SSL Protocol +TLSv1.1+>>d:\temp\sslinfo.txt

d:\micros\opera\tools\SnR /D=D:\ORA\operainstance\config\OHS\ohs1
/F=ssl.conf /A="SSLSessionCacheTimeout 300" /R=d:\temp\sslinfo.txt
/S /I
```

d:\ora\operainstance\bin\opmnctl shutdown
d:\ora\operainstance\bin\opmnctl startall

Remove TLS/SSL Ciphers with Known Weaknesses

```
Edit SSL.conf located in D:\ORA\operainstance\config\OHS\ohs1
```

Current Value SSLCipherSuite

```
SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_
CBC_SHA,SSL_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WI
TH_AES_256_CBC_SHA
```

Replacement Value

```
SSLCipherSuite RC4-
SHA:SSL_RSA_WITH_RC4_128_MD5:SSL_RSA_WITH_RC4_128_SHA
```

New Value

```
Search for ‘SSLSessionCacheTimeout 300’ and add the value shown below
it:

SSLProtocol -ALL +SSL Protocol

Save SSL.conf
```

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

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

Oracle uses separate development and production environments to ensure software integrity and security. Updated patches and security updates are available via the Oracle website, <http://www.oracle.com>.

Although OPERA Cloud uses Apache web server to distribute the application internally to your network, this server should not be used for any external web applications.

Access to this server from the internet has to be severely restricted by use of a firewall. Never keep the database server and web server on the same server for your environment.

Permissive network filtering

OPERA Cloud installation is configuring Apache to listen on port 80. This port is NOT used to access application. Application is currently accessed via HTTPS(443) port.

PCI-Compliant Remote Access (PA-DSS 10.1)

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

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

Oracle Hospitality OPERA 5 and OPERA Cloud utilize this two-factor authentication by having the user have to sign into the OPERA application itself with a User ID and Password and then another User ID and Password must be entered to get into other sections within OPERA, such as Cashiering.

And when swiping a credit card on an encrypted credit card reader from within the Payment Application (widget), OPERA will read the configuration of the credit card reader and pass this configuration information on to the Payment Application. The widget then parses the credit card information. The Expiration Date, Name of the Credit Card holder, the last 4 digits of the credit card number, and encrypted track data are extracted and sent to the Credit Card Vendor, based on the credit card reader device configuration. The Credit Card Vendor then decrypts the data and returns a token to OPERA to be used with any following credit card transactions.

Also, OPERA supports the Chip and PIN method of credit card and membership card authorization for both offline and online transactions. In addition, OPERA Kiosk supports Chip and PIN credit card payments to be made through a hotel kiosk system. Chip and PIN relies on a microchip inserted into the card; the chip stores cardholder authentication information. When the card is inserted into a specially designed reader, the microchip is accessed and the cardholder is prompted to enter a PIN (Personal Identification Number) to authorize the card.

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

OPERA Cloud 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 Cloud 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 remote access to customer networks. These are made available on the Oracle website < http://support.oracle.com > for download.

For receiving updates via remote access, merchants must adhere to the following guidelines:

Secure remote access technology use, per PCI Data Security Standard 12.3.9:

12.3 *Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use.*

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.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, Oracle Support, 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). For RDP/Terminal Services this means using the high encryption setting on the server, and for Oracle Support it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

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 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 1.1/TLS 1.2) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

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

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

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

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

OPERA Cloud 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 (PA-DSS 12.1)

OPERA Cloud or server allows non-console administration, so you must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access.

Network Segmentation

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

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

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

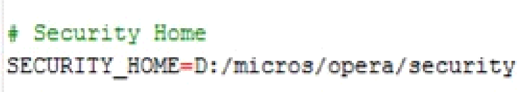
Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Possible Database or Webserver variations

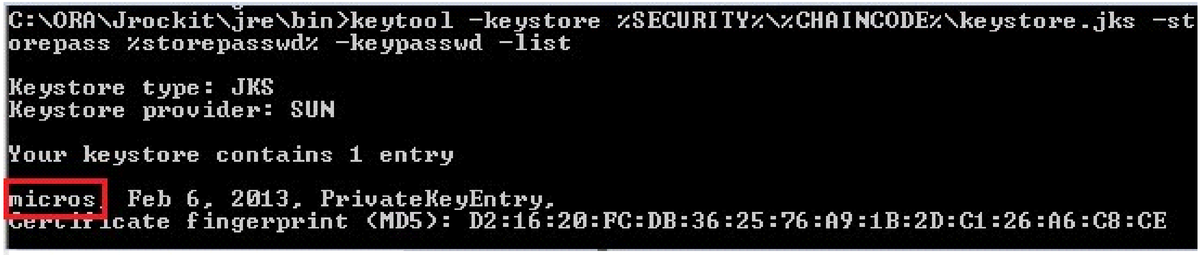
HP-UX Itanium	1 Version (11.31)
HP-UX PA-RISC (64-bit)	1 Version (11.31)
IBM AIX on POWER Systems (64-bit)	3 Versions (7.1, 6.1, 5.3)
IBM: Linux on System z	5 Versions (SLES 11, SLES 10, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 4)
Linux x86	10 Versions (SLES 11, SLES 10, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 4, Oracle Linux 6, Oracle Linux 5, Oracle Linux 4, Asianux 3, Asianux 2)
Linux x86-64	12 Versions (SLES 11, SLES 10, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 4, Oracle Linux 7, Oracle Linux 6, Oracle Linux 5, Oracle Linux 4)
Microsoft Windows x64 (64-bit)	10 Versions (Vista, 8.1, 8, 7, 2012 R2, 2012, 2008 R2, 2008, 2003 R2)
Oracle Solaris on SPARC (64-bit)	2 Versions (11, 10)
Oracle Solaris on x86-64 (64-bit)	2 Versions (11, 10)

- Sizing Document – for more information on supporting hardware sizing, see OPERA Mobility Hardware Sizing.
- TCP/IP network connectivity
- All latest updates and hot-fixes should be tested and applied

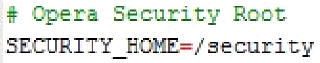
Payment Application Initial Setup & Configuration



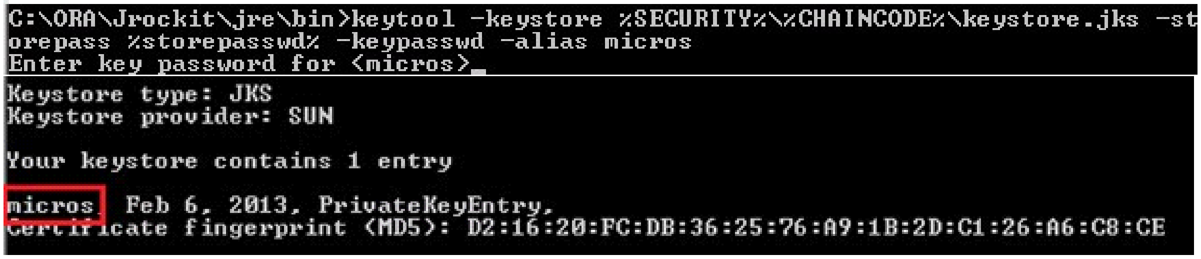
```
# Security Home
SECURITY_HOME=D:/micros/opera/security
```



```
C:\ORA\Jrockit\jre\bin>keytool -keystore %SECURITY%\%CHAINCODE%\keystore.jks -st
orepass %storepasswd% -keypasswd -list

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

micros, Feb 6, 2013, PrivateKeyEntry,
Certificate fingerprint (MD5): D2:16:20:FC:DB:36:25:76:A9:1B:2D:C1:26:A6:C8:CE
```



```
# Opera Security Root
SECURITY_HOME=/security
```

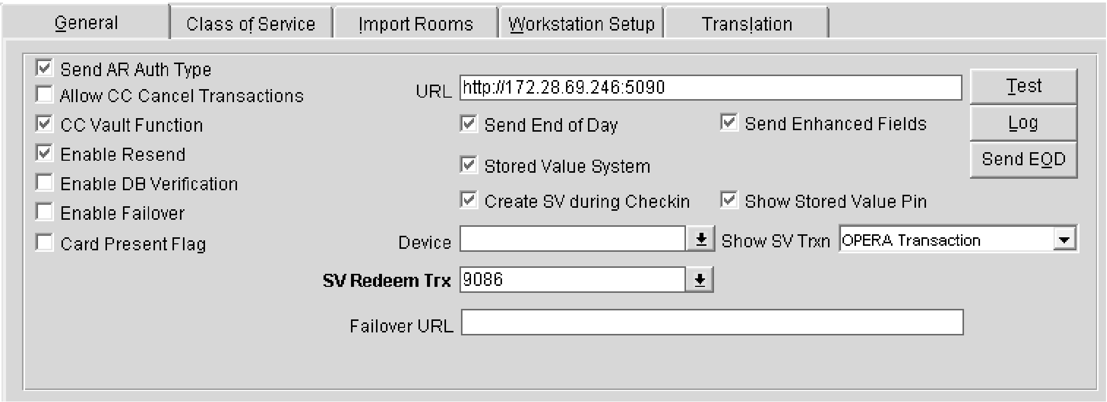


```
C:\ORA\Jrockit\jre\bin>keytool -keystore %SECURITY%\%CHAINCODE%\keystore.jks -st
orepass %storepasswd% -keypasswd -alias micros
Enter key password for <micros>_
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

micros, Feb 6, 2013, PrivateKeyEntry,
Certificate fingerprint (MD5): D2:16:20:FC:DB:36:25:76:A9:1B:2D:C1:26:A6:C8:CE
```

Defining the Payment Gateway

OPERA Cloud and OPERA Version 5 applications share the same configuration steps for setting up the Target URL for the Vendor supplying Credit Card handling services. This URL is added to the Interface Setup screen for the associated provider.

The General tabbed area appears similar to the following image when configuring CCW interfaces:



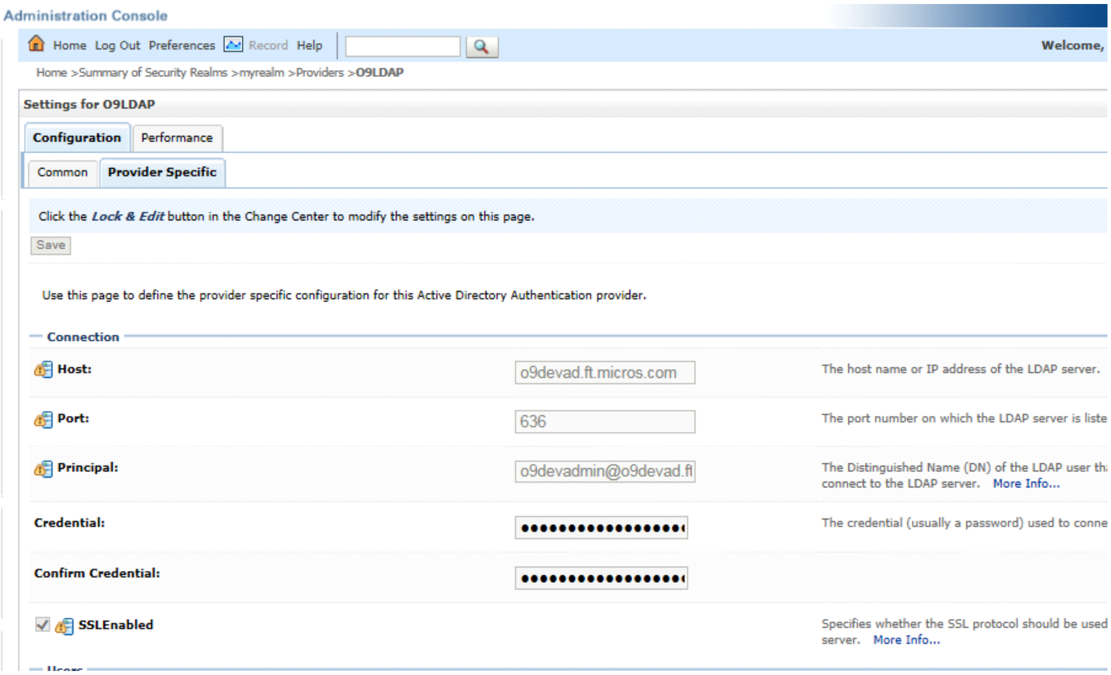
☑ Send AR Auth Type
☐ Allow CC Cancel Transactions
☑ CC Vault Function
☑ Enable Resend
☐ Enable DB Verification
☐ Enable Failover
☐ Card Present Flag

URL: http://172.28.69.246:5090
☑ Send End of Day
☑ Send Enhanced Fields
☑ Stored Value System
☑ Create SV during Checkin
☑ Show Stored Value Pin
Device:
Show SV Trxn: OPERA Transaction
SV Redeem Trx: 9086
Failover URL:

Connectivity to that URL can be tested using the Test Button on the IFC Web Interface screen.

Conducting Test Transactions

Generally the end point for the Vendor QA environment is different from that of the production environment and certificates for both may need to be imported if the vendor certificates differ. Once the end points and certificates are installed testing in the QA environment will mirror the process of testing in the Production environment. A successful test is reflected by the retention of the Vendor token that can be used to process Authorizations or Settlements in future transactions.



Click the ***Lock & Edit*** button in the Change Center to modify the settings on this page.

Use this page to define the provider specific configuration for this Active Directory Authentication provider.

Host:	o9devad.ft.micros.com	The host name or IP address of the LDAP server.
Port:	636	The port number on which the LDAP server is liste
Principal:	o9devadmin@o9devad.fi	The Distinguished Name (DN) of the LDAP user th: connect to the LDAP server. More Info...
Credential:	•••••••••••••••••••	The credential (usually a password) used to conne
Confirm Credential:	•••••••••••••••••••	
☑ **SSLEnabled**		Specifies whether the SSL protocol should be used server. More Info...

Updating your Encryption Key on a Periodic basis

Refer to the Oracle Hospitality OPERA 5 PA-DSS 3.1 Implementation Guide Release 5.0.05.01 for the approved process.

Appendix A Inadvertent Capture of PAN

This appendix provides instructions for addressing the inadvertent capture of PAN on the following supported operating systems:

- Microsoft Windows 8
- Microsoft Windows 7

Microsoft Windows 8

Disable System Restore

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

Encrypt PageFile.sys

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

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

Clear the System PageFile.sys on Shutdown

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

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

Disable System Management of PageFile.sys

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

Disable Error Reporting

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

Microsoft Windows 7

Disable System Restore

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

Encrypt PageFile.sys

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

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

Clear the System PageFile.sys on Shutdown

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

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

Disable System Management of PageFile.sys

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

Disable Error Reporting

1. Click the **Start** button, select **Control Panel**, and then click **Action Center**.
2. Click **Change Action Center settings**, then click **Problem reporting settings**.
3. Select **Never check for solutions**, then click **OK**.