Oracle® Hospitality OPERA Cloud Services

Security Guide

Release 22.5
F73198-01
January 2023

ORACLE

Oracle Hospitality OPERA Cloud Services Security Guide Release 22.5

F73198-01

Contents

Preface

Purpose

This document provides security reference and guidance for Oracle Hospitality OPERA Cloud Services.

This document is intended for:

- OPERA Customers
- Oracle Installers
- Oracle Dealers
- Oracle Customer Service
- Oracle Training Personnel
- IT Personnel

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

The following documents provide additional detail for the Payment Card Industry Data Security Standard (PCI DSS) and Open Web Application Security Project (OWASP):

PCI DSS
https://www.pcisecuritystandards.org/security_standards/index.php

Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
https://benchmarks.cisecurity.org/downloads/multiform/

For Oracle products documentation, visit the Oracle Help Center website at http://docs.oracle.com.

Revision History

Date	Description of Change
January 2023	Initial publication

1

OPERA Cloud Security Overview

This chapter provides an overview of Oracle Hospitality OPERA Cloud Services (OPERA Cloud) security and explains the general responsibilities of both the customer and Oracle.

Customer Responsibilities

At a high level, customers are responsible for:

- Understanding Oracle's security policies.
- Implementing their own corporate policies via Oracle tools.
- Creating and administering users via Oracle tools.
- Ensuring data quality and enforcing end-user devices security controls, so that antivirus, malware and other malicious code checks are performed on data and files before uploading data.
- Ensuring that end-user devices meet the minimum security requirements.
  - For information on browser security, visit https://us-cert.cisa.gov/publications/securing-your-web-browser
- Generating public/private key pairs as requested by OPERA Cloud

To securely implement OPERA Cloud Service, customers and their implementation partners should read this document to understand Oracle's security policies. This document summarizes information and contains links to many other Oracle documents.

Oracle Responsibilities

As the cloud service provider, at the highest level Oracle is responsible for:

- Building secure software.
- Provisioning and managing secure environments.
- Protecting the customer’s data.

OPERA Cloud Service fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. Sections in this document will describe this information in great detail later in this document.

2 Oracle OPERA Cloud SaaS Security

Security is a many faceted issue to address. To discuss Oracle SaaS security, it helps to define and categorize the many aspects of security. For the purposes of this document, we discuss the following categories of SaaS security:

- Secure Product Engineering
- Secure Deployment
- Secure Management Assessment and Audits

Secure Product Engineering

Oracle builds secure software through a rigorous set of formal, always evolving security standards and practices known as Oracle Software Security Assurance (OSSA). OSSA encompasses every phase of the product development lifecycle.

More information about OSSA can be found at:
https://www.oracle.com/corporate/security-practices/assurance/

The cornerstones of OSSA are Secure Coding Standards and Security Analysis and Testing.

Secure Coding Standards include both general use cases and language specific security practices. More information about these practices can be found at:

https://www.oracle.com/corporate/security-practices/assurance/development/

Security Analysis and Testing includes product specific functional security testing and both static and dynamic analysis of the code base. Static Analysis is performed via tools including both internal Oracle tools and Fortify. Dynamic Analysis focuses on APIs and endpoints, using techniques like fuzzing to test interfaces and protocols.

https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html

Specific security details of the Merchandising Cloud Service are discussed in detail later in this document.

Secure Deployment

Secure deployment refers to the security of the infrastructure used to deploy the SaaS application. Key issues in secure deployment include Physical Safeguards, Network Security, Infrastructure Security and Data Security.

Physical Safeguards

Oracle SaaS applications are deployed via Oracle Cloud Infrastructure datacenters. Access to Oracle Cloud data centers requires special authorization that is monitored and audited. The premises are monitored by CCTV, with entrances protected by physical barriers and security guards. Governance controls are in place to minimize the resources that are able to access systems. Physical security safeguards are further detailed in Oracle's Cloud Hosting and Delivery Policies.

http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf

Network Security

The Oracle Cloud network is isolated from the Oracle Corporate Network. Customer instances are separated down to the VLAN level.

Infrastructure Security

The security of the underlying infrastructure used to deploy Oracle SaaS is regularly hardened. Critical patch updates are applied on a regular schedule. Oracle maintains a running list of critical patch updates and security alerts. Per Oracle's Cloud Hosting and Delivery Policies, these updates are applied to all Oracle SaaS systems.

https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Before Oracle deploys code to SaaS, Oracle's Global Information Security team performs penetration testing on the cloud service. This penetration testing and remediation prevents software or infrastructure issues in production systems.

https://www.oracle.com/corporate/security-practices/assurance/development/ethical-hacking.html

Data Security

Oracle uses a number of strategies and policies to ensure the customer’s data is fully secured.

- Data Design - Oracle applications avoid storing personal data. Where PII data exists in a system, Data Minimization, Right to Access and Right to forget services exist to support data privacy standards.
- Storage - Oracle applications use encrypted tablespaces to store sensitive data.
- Transit - All data is encrypted in transit, SaaS uses TLS for secure transport of data, as documented in Oracle's Cloud Hosting and Delivery policy. https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf

Secure Management

Oracle manages SaaS based on a well-documented set of security-focused Standard Operating Procedures (SOPs). The SOPs provide direction and describe activities and tasks undertaken by Oracle personnel when delivering services to customers. SOPs are managed centrally and are available to authorized personnel through Oracle's intranet on a need-to-know basis.

All network devices, servers, OS, applications and databases underlying Oracle Cloud Services are configured and maintain auditing and logging. All logs are forwarded to a Security Information and Event Management (SIEM) system. The SIEM is managed by the Security Engineering team and is monitored 24*7 by the Security Operations team. The SIEM is configured to alert the Security Operations team regarding any conditions deemed to be potentially suspicious, for further investigation. Access given to review logs is restricted to a subset of security administrators and security operations personnel only.

3

Understanding the OPERA Cloud Environment

OPERA Cloud Implementation Planning

When planning your OPERA Cloud implementation, consider the following:

- Which resources need protection?
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?
  - For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. Analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What will happen if protections on a strategic resource fail?
  - In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understand the security ramifications of each resource and protect it properly.

Oracle provides functionality within the OPERA application for Personal Information (that is passport, date of birth, and credit card). Placing this information in fields other than the designated areas, such as Notes or Comments fields, is open for PCI review and does not comply with PCI-DSS rules and regulations.

Assessment and Audit

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 the actual server (or hosting) environment called the Cardholder Data Environment (CDE). It is Oracle's responsibility as the merchant, and as your SaaS provider to work together with you (the customer) to use PCI compliant architecture with proper hardware & software configurations and access control.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.

Properly Train and Monitor Admin Personnel

It is the customer's and Oracle's 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.

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).

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.

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

OPERA Cloud 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.

4

Appendix A: Secure Deployment Checklist

The following security checklist provides guidelines that help secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access.
- Apply all security patches and workarounds.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.
  - Encrypt network traffic.
  - Harden the operating system.