Oracle Hospitality OPERA Cloud Distribution

Security Guide

Release 23.1
F74531-01
January 2023

ORACLE

Oracle Hospitality OPERA Cloud Distribution Security Guide, Release 23.1

F74531-01

Contents

1 Overview

2 OPERA Cloud Distribution SaaS Security

3 Customer Responsibilities

4 Oracle Responsibilities

5 Accessing OPERA Cloud Distribution Platform

6 Payment Card Industry (PCI) Standards

7 Personal Information

8 Properly Train and Monitor Administrators

9 Retrieving Information from OPERA Cloud APIs

10 General Security Principles

Preface

This document provides security references and guidance for Oracle Hospitality OPERA Cloud Distribution.

Audience

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
- Screen shots 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/

Oracle Hospitality product documentation is available on the Oracle Help Center.

Table Revision History

Date	Description of Change
January 2023	Initial publication.

1 Overview

This section gives an overview of OPERA Cloud Distribution cloud service security and explains the general principles of application security.

2

OPERA Cloud Distribution SaaS Security

Security is a multi-faceted issue to address. For Oracle SaaS security, it helps to define and categorize the many aspects of security. This document addresses 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 using tools including both internal Oracle tools and Fortify. Dynamic Analysis focuses on APIs and endpoints, using techniques like fuzzing to test interfaces and protocols. For more information, see: https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html.

Specific security details of OPERA Cloud Distribution 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 from Oracle Cloud Infrastructure Regional data centers. 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.

Network Security

The Oracle Cloud network is isolated from the Oracle Corporate Network. OPERA Cloud Distribution services run in a dedicated network segment of the Oracle Cloud.

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.

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 table spaces 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.

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
Customer Responsibilities

At a high level, customers are responsible for the following:

- Understanding Oracle's security policies.
- Implementing their own corporate policies using Oracle tools.
- Creating and administering users using 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

4

Oracle Responsibilities

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

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

OPERA Cloud Distribution cloud service fulfills its responsibilities using a combination of corporate level development practices and cloud delivery policies. Sections in this document describe this information in greater detail.

5

Accessing OPERA Cloud Distribution Platform

Customers access the OPERA Cloud Distribution application from the following interfaces:

- **A web browser**. This is the primary means to access all OPERA Cloud Distribution functionalities.
- **REST API**. OPERA Cloud Distribution publishes a rich set of APIs for integration with the Oracle Hospitality Integration Platform (OHIP), partners, or channels. Applications can integrate with OHIP to consume OPERA Cloud Distribution features.

The Security Model

OPERA Cloud Distribution cloud security requirements arise from the need to protect customer data from unauthorized attempts to access or alter the data. Secondary concerns include protecting against undue delays in accessing or using data, or even against interference to the point of denial of service.

The critical security features that provide these protections are:

- **Authentication**. Ensuring that only authorized individuals get access to the system and data
- **Authorization**. Access control to system privileges and data. This builds on authentication to ensure that individuals only get appropriate access.
- **Audit**. Allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.

Configuring and Using Access Control

OPERA Cloud Distribution uses the Oracle OPERA Identity Management (OIM) system for application user identity and access management. User accounts must be created in the identity management system and granted distribution specific roles to access the user interface. Review product documentation for a list of roles required to access OPERA Cloud Distribution functionalities. Oracle recommends that users use a complex password meeting federal password complexity guidance and follow principles of least privilege when assigning application roles to end-users.

Transport Layer Security

OPERA Cloud Distribution application interfaces are secured by Transport Layer Security (TLS) version 1.2 or above using only strong ciphers. This application does not support unsecured / plain HTTP communication.

On connecting to OPERA Cloud Distribution APIs, applications must validate that the TLS certificate is legitimate and not a forgery. This prevents fraudulent attacks resulting in compromised passwords and extraction of customer data.

6

Payment Card Industry (PCI) Standards

Although OPERA Hospitality Distribution does not accept customer card data directly, some APIs still let you send cardholder data, so OPERA Cloud Distribution is in scope for Payment Card Industry Data Security Standard (PCI DSS). Applications sending client systems are also in scope for PCI DSS and must follow these guidelines:

Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS).

Payment Card Industry Data Security Standard (PCI DSS).

PCI Requirements

OPERA Cloud Distribution follows these standards:

- Build and maintain a secure network and systems.
  - Install and maintain a firewall configuration to protect cardholder data.
  - Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data.
  - Protect stored cardholder data.
  - Encrypt transmission of cardholder data across open, public networks.
- Maintain a vulnerability management program.
  - Protect all systems against malware and regularly update anti-virus software or programs.
  - Develop and maintain secure systems and applications.
- Implement strong access control measures.
  - Restrict access to cardholder data by business need-to-know.
  - Identify and authenticate access to system components.
  - Restrict physical access to cardholder data.
- Regularly monitor and test networks.
  - Track and monitor all access to network resources and cardholder data.
  - Regularly test security systems and processes.
- Maintain an information security policy.
  - Maintain a policy that addresses information security.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

OPERA Cloud Distribution does not store sensitive authentication data, and Oracle strongly recommends against storing sensitive authentication data. However, if you store sensitive authentication data, you must adhere to the following guidelines when dealing with sensitive

authentication data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data 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 sensitive authentication data while stored.
- Securely delete such data immediately after use.

Secure Deletion of Cardholder Data (PA-DSS 2.1)

Any cardholder data received by OPERA Cloud Distribution is stored in a secure database. All sensitive data in the database is encrypted by default. All data is purged by the application periodically per PA-DSS v3.2.

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

OPERA Cloud Distribution must not be accessed using wireless technologies. However, should any systems downstream of the client system implement wireless access to the client system, you must adhere to the following guidelines for secure wireless settings to ensure cardholder data is secure end–to–end per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

PCI DSS section 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 any traffic (if such traffic is necessary for business purposes) from the wireless environment into the cardholder data environment.

PCI DSS section 2.1.1: Change wireless vendor defaults as follows:

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

PCI DSS section 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.

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

Never store cardholder data on Internet-accessible systems. For example, a web server and a database server must not be on same server.

Maintain an Information Security Program

In addition to the security recommendations included in this document, 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 basic plan every owner of a client system 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.

7

Personal Information

To ensure Oracle can contact you about your integrations, Oracle requires you to supply basic contact details, such as: Name, Company Name, Email Address, and Phone Number.

If you would like a copy of your data or would like your data corrected, you can request it at My Oracle Support.

Oracle requires contact details for each integration. To remove your contact details, make your request at My Oracle Support. Remember to include your Name, Company Name, Email Address, and Phone Number for the new nominated contact for that integration.

These contact details are permanently deleted when access to the OPERA Cloud Distribution APIs is terminated.

Personal Information in Log Files

OPERA Cloud Distribution and Oracle Hospitality API logs are written in a standard format and stored in standard locations with timestamps. Operational logs are sent to a shared log store in Oracle Cloud, which is subject to role-based access control.

In line with the Services Privacy Policy, Oracle is legally obligated to retain operational log file information for 90 days after which logs are automatically purged.

Assigning a Unique ID to Each Person with Computer Access

Oracle Corporation recognizes the importance of establishing unique IDs for each person with computer access. No two OPERA Cloud Distribution users can have the same ID, and each person's activities can be traced provided the customer and integrator maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis.

While Oracle Corporation makes every possible effort to conform to Requirement 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for non-consumer users and administrators for all system components depend on customer/partner specific protocol and practices.

To ensure strict access control of OPERA Cloud Distribution, always assign unique user names and complex passwords to each account. Oracle Corporation mandates applying these guidelines to not only Oracle Corporation passwords, but to passwords for systems accessing OPERA Cloud Distribution APIs and downstream of there, including server operating system passwords and end user Windows® passwords. Furthermore, Oracle Corporation advises users to control access through unique user names and PCI-compliant complex passwords to any PCs, servers, and databases with payment applications and cardholder data.

8

Properly Train and Monitor Administrators

It is the responsibility of the owner of the client system accessing OPERA Cloud Distribution APIs to institute proper personnel management techniques for allowing administration user access to cardholder data, site data, and so on. For example, the client system owner controls whether each individual administration user can see full credit card Primary Account Numbers (PAN) or only the last four digits of the PAN.

In most systems, a security breach is often the result of unethical personnel, so pay special attention to whom you trust with admin access and whom you allow to view fully decrypted and unmasked payment information.

When administering the OPERA Cloud Distribution services, Oracle Cloud Operations always use multi-factor authentication (MFA) using physical tokens to access production instances of OPERA Cloud Distribution.

9

Retrieving Information from OPERA Cloud APIs

OPERA Cloud Distribution APIs always respond with content in `application/json` format. If requests are not made in `application/json` format, OPERA Cloud Distribution APIs may return plain text error responses.

Applications should ensure any data returned from OPERA Cloud Distribution APIs is managed securely and safely. The system should:

- Encrypt any sensitive data. Data returned from OPERA Cloud Distribution APIs may contain personal and other sensitive information. If your client system needs to store this information, it should be stored securely and encrypted within the data store. Access to the data should be restricted and accounts should have minimum access rights to the data in order to prevent elevated access.
- Any data output to users from an OPERA Cloud Distribution API response should be sanitized to ensure there is no possibility of cross-site scripting.
- Validate all data received from the OPERA Cloud Distribution APIs.

10

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Throughout this document, Oracle assumes that all security patches are applied to the operating system and the web browser accessing the OPERA Cloud Distribution user interface.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. The overly ambitious granting of responsibilities, roles, grants, and so on, especially early in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Keep Up To Date on Latest Security Information

Build your applications with secure coding practices in mind. Oracle recommends any software built to connect to OPERA Cloud Distribution be assessed to avoid the security flaws described by the OWASP Top Ten Project.

While some of the advice may not seem relevant to a server that is calling the OPERA Cloud Distribution interface, the advice also applies to any devices that connect to your server.