# Oracle Hospitality OPERA Reporting and Analytics Cloud Service

## Security Guide

G11728-01
July 2024

Oracle Hospitality OPERA Reporting and Analytics Cloud Service Security Guide,

G11728-01

# Contents

# Preface

Oracle Hospitality OPERA Reporting and Analytics Cloud Service is a web-based application that centralizes hotel property management data to provide operational and analytical insights into business operations, and to improve efficiency by delivering information to all roles within an organization.

### Purpose

This document provides security reference and guidance for Oracle Hospitality OPERA Reporting and Analytics Cloud Service (OPERA R&A).

### Audience

This document is intended for.

- OPERA R&A 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 document provides additional detail for Open Web Application Security Project (OWASP):

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 at http://docs.oracle.com.

## Revision History

### Table 1 Revision History

| Date | Description of Change |
|---|---|
| July 2024 | Initial Publication |

# 1 OPERA R&A Security Overview

This chapter provides an overview of Oracle Hospitality OPERA Reporting and Analytics Cloud Service (OPERA R&A) 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 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
- Generating public/private key pairs as requested by OPERA R&A

To securely implement OPERA R&A, 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 R&A fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. This document will describe this information in great detail.

# 2 Oracle OPERA R&A 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 purpose 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 using 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 R&A Implementation Planning

When planning your OPERA R&A 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.

Personal information cannot be entered directly into OPERA R&A. Oracle provides functionality within OPERA for personal information that is shared with OPERA R&A. Placing personal information in OPERA fields other than the designated areas, such as Notes or Comments fields, does not comply with regulations for data protection.

## Assessment and Audit

**Build and Maintain a Secure Network and Systems**

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

**Maintain a Vulnerability Management Program**

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

**Implement Strong Access Control Measures**

- Identify and authenticate access to system components.

**Regularly Monitor and Test Networks**

1. Track and monitor all access to network resources.

2. Regularly test security systems and processes.

**Maintain an Information Security Policy**

- 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 personal data, site data, etc.

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 personal information in specific fields on the user interface. The form fields that are intended to receive this information are clearly labeled. Some are designed with heightened security controls such as data masking in the form and encryption of at rest in OPERA.

Entering this personal information in any other OPERA field (for example, in a Notes or Comments field), does not provide it with these heightened security controls.

OPERA R&A provides heightened security controls that allow for the inclusion or exclusion of personal or sensitive personal information in all reporting. Personal Information is protected under a single privilege while sensitive personal information is protected by another. See Appendix B for additional details.

A

# 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.

B

# Appendix B: Personally Identifiable Information

The following types of personally identifiable information may have been received by OPERA R&A for use in reporting. A unique permission is available to allow users to view personal information in either of these categories.

**Table B-1 Personal Information**

| Personal Information | Sensitive Personal Information |
|---|---|
| Personal details (e.g., name, date of birth, gender, marital status, number of children and name(s)); | Government identification (e.g., National ID/Passport details/Social Security Number, Driver’s License) |
| Personal contact details (including home address, home telephone or mobile number, email address, and passwords) | |
| Professional contact details (e.g., work phone number and email and physical address) | |
| Employee ID | |
| Customer ID | |
| Customer account information | |

Instructions to provide users with permission to include this data in reporting can be found under the Groups, Permissions and Users section of the OPERA Reporting and Analytics User Guide.