

Oracle® Hospitality OPERA Cloud Services

Security Guide



Release 26.4
G58712-01
September 2026

ORACLE®

Copyright © 2017, 2026, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	iv
1 OPERA Cloud Security Overview	1-1
Customer Responsibilities	1-1
Oracle Responsibilities	1-1
2 Oracle OPERA Cloud SaaS Security	2-2
Secure Product Engineering	2-2
Secure Deployment	2-3
3 Understanding the OPERA Cloud Environment	3-1
OPERA Cloud Implementation Planning	3-1
Assessment and Audit	3-2
Properly Train and Monitor Admin Personnel	3-4
PCI DSS v4.0.1-Compliant Wireless Settings	3-5
Protection of Account Data in End User Messaging Technologies	3-5
4 Appendix A: Secure Deployment Checklist	4-1

Preface

Purpose

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

This guide uses PCI DSS v4.0.1 as the current payment-card security baseline. PCI DSS applies to entities that store, process, or transmit cardholder data or sensitive authentication data, and to systems that could affect the security of the cardholder data environment. Customers remain responsible for determining their PCI DSS scope and validating compliance with their acquirer, payment brands, or Qualified Security Assessor.

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 Customer Support Portal at the following URL:

<https://iccp.custhelp.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 v4.0.1: <https://www.pcisecuritystandards.org/standards/pci-dss/>

PCI SSC Document Library: https://www.pcisecuritystandards.org/document_library/

PCI DSS v4.0.1 publication and selected changes:

<https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1>

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
February 2025	Release 25.1: Initial publication.
February 2025	Release 25.2: Minor editorial corrections and publication-number update. No substantive security-control changes.
May 2025	Release 25.3: Updated release metadata and publication number. No substantive security guidance changes.
August 2025	Release 25.4: Updated release metadata, publication date, and publication number. No substantive security guidance changes.
October 2025	Release 25.5: Administrative publication. The published document duplicated Release 25.4 content and metadata; corrected in a subsequent release.
January 2026	Release 26.1: Updated release metadata, publication date, and copyright year. No substantive security guidance changes.
February 2026	Release 26.2: Updated release metadata and publication date. No substantive security guidance changes.
May 2026	Release 26.3: Updated release metadata and publication date. No substantive security guidance changes.
September 2026	Release 26.4: Aligned the guide with PCI DSS v4.0.1. Updated PCI references and terminology; clarified critical vulnerability remediation, payment-page script management, phishing-resistant authentication, PAN protection, and customer and third-party service provider responsibilities; added current applicability dates and glossary terms; and removed the retired PA-DSS reference.

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://www.cisa.gov/news-events/news/evaluating-your-web-browsers-security-settings>
- Generating public/private key pairs as requested by OPERA Cloud

Determining the customer cardholder data environment, PCI DSS scope, and applicable validation method.

Managing customer-controlled users, endpoints, integrations, payment providers, and third-party service providers in accordance with PCI DSS v4.0.1.

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.

Providing applicable service-provider security controls and compliance evidence for the Oracle-managed service.

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 issues 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 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.

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

Specific security details of the 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.

https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf?download=false

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. PCI DSS v4.0.1 requires critical security patches and updates for applicable in-scope system components to be installed within one month of release. Other security vulnerabilities are addressed according to documented risk rankings and remediation timelines. Oracle applies security updates to Oracle-managed SaaS systems in accordance with Oracle's Cloud Hosting and Delivery Policies. Customers remain responsible for customer-managed endpoints, integrations, networks, and third-party components within their PCI DSS scope.

<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/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf?download=false

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

PCI DSS v4.0.1 provides baseline technical and operational requirements for protecting payment account data. It applies to entities that store, process, or transmit cardholder data or sensitive authentication data, and to systems that could affect the security of the cardholder data environment (CDE). Oracle operates OPERA Cloud as a service provider; customers are responsible for determining their complete PCI DSS scope and validation obligations. Oracle, customers, and applicable third-party service providers must coordinate their responsibilities for the shared environment.

PCI DSS v4.0.1 Applicability and Effective Dates

PCI DSS v4.0.1 was published on June 11, 2024 as a limited revision that clarified requirements and guidance without adding or deleting requirements. PCI DSS v4.0 was retired on December 31, 2024, after which v4.0.1 became the only active PCI DSS v4 version supported by PCI SSC. The future-dated PCI DSS v4.x requirements became effective on March 31, 2025.

Build and Maintain a Secure Network and Systems

- Install and maintain network security controls.
- Apply secure configurations to all system components.

Protect Account Data

- Protect stored account data.
- Protect cardholder data with strong cryptography during transmission over open, public networks.

Maintain a Vulnerability Management Program

- Protect all systems and networks from malicious software.
- Develop and maintain secure systems and software.

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

- Log and monitor all access to system components and cardholder data.
- Test security of systems and networks regularly.

Maintain an Information Security Policy

- Support information security with organizational policies and programs.

Vulnerability and Patch Management

Critical security patches and updates for applicable in-scope system components must be installed within one month of release. Other vulnerabilities must be prioritized and remediated according to documented risk rankings and organizational remediation

timelines. Responsibilities must be assigned for Oracle-managed services, customer-managed components, and external provider components.

Payment-Page Scripts

Where payment-page scripts are used, the responsible party must maintain an inventory, authorize each script, document its business justification, validate script integrity, and detect unauthorized additions or changes. Oracle, customer, and external payment-provider responsibilities depend on who supplies, hosts, configures, or can modify the script.

Authentication

Multi-factor authentication must be implemented where required for access into the CDE. The PCI DSS v4.0.1 applicability exception for non-administrative access applies only when an account is authenticated exclusively with phishing-resistant authentication factors. Passwords, one-time passcodes, and ordinary push approvals must not be treated as phishing-resistant without appropriate validation.

PAN Protection

If keyed cryptographic hashes are used to render Primary Account Numbers (PAN) unreadable, the implementation must meet the applicable PCI DSS v4.0.1 objective and key-management requirements. Hash keys must be protected and managed separately from the protected data. If OPERA Cloud does not use keyed cryptographic hashes for this purpose, the control must be documented as not applicable rather than assumed.

Customer and Third-Party Service Provider Responsibility Matrix

The following responsibility summary is a guide. Contractual documents, service descriptions, and current compliance evidence remain authoritative.

Account and access management

Oracle: Oracle service and platform accounts.

Customer: Users, roles, access reviews, and termination.

External provider: Provider accounts and access.

Network security and connectivity

Oracle: Cloud infrastructure and service boundaries.

Customer: Customer networks, endpoints, and connectivity.

External provider: Provider connectivity and services.

Payment-page script management

Oracle: Oracle-supplied or operated scripts.

Customer: Customer-added scripts and integrations.

External provider: Provider-supplied scripts.

Vulnerability remediation

Oracle: Oracle-managed components.

Customer: Customer-managed systems and integrations.

External provider: Provider-managed components.

Logging and monitoring

Oracle: Service and infrastructure logs.

Customer: Activity, user, endpoint, and integration logs.

External provider: Provider logs and alerts.

Incident response coordination

Oracle: Oracle-managed service incidents.

Customer: Customer procedures and required notifications.

External provider: Provider-service incidents.

Compliance evidence

Oracle: Service-provider compliance evidence.

Customer: Validate scope and retain evidence.

External provider: TPSP compliance evidence.

PCI DSS Terminology

Cardholder Data Environment (CDE): The people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data, and systems that could affect their security.

Primary Account Number (PAN): The defining account number for a payment card account.

Sensitive Authentication Data (SAD): Security-related information used to authenticate cardholders or authorize payment transactions.

Third-Party Service Provider (TPSP): A third party that stores, processes, or transmits account data or could affect the security of the CDE.

Phishing-Resistant Authentication: Authentication designed to prevent disclosure and use of authentication secrets through phishing.

Payment Page: A web-based user interface containing one or more form elements intended to capture account data.

Legal Exception and Visitor: Use the current definitions in the PCI SSC glossary when these terms apply.

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 DSS v4.0.1-Compliant Wireless Settings

Where wireless technologies are used with OPERA Cloud or within the CDE, the following secure settings must be implemented in accordance with applicable PCI DSS v4.0.1 requirements 1.3.3, 2.3.1, and 4.2.1.2:

PCI DSS 1.3.3: 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 2.3.1: For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:

- Default wireless encryption keys.
- Passwords on wireless access points.
- SNMP defaults.
- Any other security-related wireless vendor defaults.

PCI DSS 4.2.1.2: Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

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

Protection of Account Data in End User Messaging Technologies

Unprotected PAN, sensitive authentication data, authentication credentials, and other sensitive payment information must not be sent through end-user messaging technologies such as email, instant messaging, SMS, chat, or fax. OPERA Cloud masks PAN on materials that can be printed, emailed, or faxed so that the PAN is not readable by a person viewing the item.

Where transmission of PAN through an end-user messaging technology is explicitly authorized, the data must be protected with strong cryptography in accordance with applicable PCI DSS v4.0.1 requirements and organizational policies.

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 critical security patches within one month and remediate other vulnerabilities according to documented risk-based timelines.

- Implement and maintain effective network security controls.
- Authorize, document, and restrict all network-security-control exceptions.
- Protect the Oracle listener.
- Monitor listener activity.
- Monitor who accesses your systems.
- Check network IP addresses.
- Encrypt network traffic.
- Harden the operating system.