Oracle® Hospitality Nor1 Cloud Services

Security Guide

Release 23.1
F84883-02
June 2024

Oracle Hospitality Nor1 Cloud Services Security Guide, Release 23.1

F84883-02

Contents

1 Oracle Nor1 Cloud Security Overview

Oracle Responsibilities 1-1
Customer Responsibilities 1-1

2 Oracle Nor1 Cloud SaaS Security

Secure Product Engineering 2-1
Secure Deployment 2-1
- Data Security 2-1
- Cookies Policy 2-2

3 Understanding Nor1 Cloud Services

Nor1 Implementation Planning 3-1
Assessment and Audit 3-1
Properly Train and Monitor Admin Personnel 3-2

4 Appendix A: Secure Operating Environment Checklist

Preface

This document provides security reference and guidance for Oracle Hospitality Nor1 Cloud Services.

Purpose

This guide explains how to work with the Nor1 Security Solutions.

Customer Support

The following support options are available:

- Live Chat is provided for Nor1 CheckIn Merchandising customers directly in the application.
- Nor1 eStandby Upgrade support is provided on the Customer Support Portal at the following URL: https://iccp.custhelp.com.
- Customers can contact their Account Relationship team or Account Revenue Manager directly.

When contacting Customer Support, please provide the following:

- Product and program/module name.
- Functional and technical description of the problem (include business impact).
- Detailed step-by-step instructions to be re-created.
- 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/
- For Oracle products documentation, visit the Oracle Help Center website: http://docs.oracle.com.
- Oracle Hotels Portal: https://docs.oracle.com/en/industries/hospitality/hotels.html

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/.

Revision History

Table Revision History

Date	Description of Change
June 2024	Added Cookies Policy statement in the following locations: • Secure Deployment • Properly Train and Monitor Admin Personnel

1

Oracle Nor1 Cloud Security Overview

This chapter provides an overview of Oracle Hospitality Nor1 Cloud Services security and explains the general responsibilities of both the customer and Oracle.

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

In accordance with reasonable practices, Oracle provides secured computing facilities for both office locations and production Cloud infrastructure.

Oracle Hospitality Nor1 Cloud Services fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. Sections in this document describe this information in greater detail.

Customer Responsibilities

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

- Understanding Oracle security policies.
- Implementing their own corporate policies from Oracle tools.
- Understanding related Oracle Hospitality Security Guides located on the Oracle Hotels Portal at https://docs.oracle.com/en/industries/hospitality/hotels.html.
- 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 Cloud.

To securely implement Oracle Hospitality Nor1 Cloud Services, 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.

2

Oracle Nor1 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. This document addresses the following categories of Software as a Service (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.

You can find more information about OSSA 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. You can find more information about these practices at: Coding Standards.

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. You can find more information at: Oracle Corporate Security Practices.

Specific security details of Oracle Hospitality Nor1 Cloud Services are addressed 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.

In accordance with reasonable practices, Oracle provides secured computing facilities for both office locations and production cloud infrastructure.

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 personally identifiable 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.

Cookies Policy

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

3
Understanding Nor1 Cloud Services

Nor1 Implementation Planning

When planning your Oracle Hospitality Nor1 Cloud Services implementation, consider the following:

- Which resources need protection?
  - You need to protect customer data.
  - 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 workflow 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.

For sensitive 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 audit reviews and may not comply with rules and regulations.

Assessment and Audit

It is important to maintain a policy that protects sensitive data such as Personally Identifiable Information and Payment Card Industry (PCI) information when running the network.

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

1. Protect stored cardholder data.
2. Encrypt transmission of cardholder data across open, public networks.

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

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

1. 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 sensitive personally identifiable data, cardholder data, site data, and so on.

In most systems, a security breach is the result of unethical personnel. Pay special attention to whom you trust into your admin site and whom you allow to view fully decrypted and unmasked sensitive personally identifiable data or payment information.

Sensitive personal information (including passport, date of birth, and credit card numbers) must be entered 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 data 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 this type of data.

Cookies Policy

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

4

Appendix A: Secure Operating Environment Checklist

The following security checklist provides guidelines that can help secure your operating environment. It is applicable to both your Oracle Hospitality Nor1 Cloud Services solution and on-premise Property Management Systems (PMS):

- Install and/or configure 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 penetrate through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.
  - Use Allow List for IP addresses.
  - Encrypt network traffic.
  - Harden the operating system.