Oracle Hospitality Payment Interface
Release Notes

Release 20.4

F95668-01

June 2024

ORACLE®

Oracle Hospitality Payment Interface Release Notes Release 20.4

F95668-01

Contents

Preface

This document describes the features and updates included in the Oracle Payment Interface (OPI) Release 20.4.

Purpose

These Release Notes provide a brief overview of additions, enhancements, and corrections implemented in this software release. Their intent is informative, not instructional. Review the Oracle Payment Interface product documentation, including technical and application advisories for previous versions, for detailed information on installation, upgrade, configuration, and general use.

Audience

This document is intended for customers who install and use Oracle Payment Interface 20.4.

Customer Support

To contact Oracle Customer Support, access the 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
- Screen shots of each step you take

Documentation

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

http://docs.oracle.com/en/industries/hospitality/

Table 1-1 Revision History

Date	Description
June 2024	• Initial Publication.

1
System Requirements, Supported Systems, and Compatibility

The Oracle Payment Interface release 20.4 is compatible with the following operating systems:

- Microsoft Windows 10 Professional
- Microsoft Windows 10 Enterprise
- Microsoft Windows 11 Professional
- Microsoft Windows 11 Enterprise
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Only supports 64bit Operating System

Oracle Hospitality OPERA Property Management System

The Oracle Payment Interface is supported for the following minimum OPERA Property Management Systems releases:

- OPERA On Premise 5.5.0.24.4 or higher
- OPERA On Premise with Multi-Property 5.5.0.25.8 or higher
- OPERA V5 Hosted 5.5.0.25.8 or higher
- OPERA V5.6.6 or higher
- OPERA Cloud 1.20.16 or higher
- OPERA Cloud 19.4 or higher

For customers running OPERA Cloud, and using the OPERA V5.5 front end, V5.5.25.8 is the minimum.

Oracle Hospitality Shipboard Property Management System

The Oracle Payment Interface is supported for the following Shipboard Property Management Systems releases:

- 8.0.17 and higher

Oracle Hospitality Suite8 Property Management System

The Oracle Payment Interface is supported for the following Suite8 Property Management Systems releases:

- 8.12.0.0 and higher

2
Resolved Issues

The following customer-reported issues were resolved in this release:

> **NOTE:**
>
> This release has upgraded third-party software components.

Table 2-1 – Resolved Issues

BugDB	JIRA	Product	Description
36349797	HPI-1601	OPI Core	In previous releases, OPI had an issue processing UTF8 characters in messages in some cases. The issue has been resolved in this release.
35697869	HPI-1582	OPI Core	Support of certificates created with OpenSSL v3 is now included in this release.
36496413	HPI-1606	OPI Installation/Upgrade	This release has addressed some upgrade issues reported in previous versions.

32082785	HPI-1275	OPI Installation/Upgrade	The updated ciphers list for the OPI service in the TLS 1.2 protocol is given below:

Existing Ciphers Supported:
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Added Ciphers Supported:
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Deprecated Ciphers:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

BugDB	JIRA	Product	Description
			TLS_DHE_RSA_WITH_AES_256_ GCM_SHA384
36549847	HPI-1613	OPI Configuration	Fixed an issue causing the GoDaddy root certificate to display an error message during import.
36534628	HPI-1611	OPI Configuration	Self-Signed certificates created by OPI Configuration include the subjectAlternativeName extension for products that require it during validation.

Refer to the ReadMe files attached to patch sets and interim patches for additional bug fixes.