

Oracle® Hospitality OPERA Property Management
Security Guide
Release 5.6.4 and higher
F18432-03

May 2023

Copyright © 1987, 2020, 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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 | 1-A |
| Audience | 1-A |
| Customer Support..... | 1-A |
| Related Documentation..... | 1-A |
| PCI Security Standards Council Reference Documents..... | 1-A |
| Revision History..... | 1-B |
| 1 OPERA Property Management Security Overview..... | 1-1 |
| Basic Security Considerations | 1-1 |
| Overview of OPERA Property Management Security..... | 1-2 |
| OPERA Property Management Network..... | 1-2 |
| OPERA Property Management Database Server Components..... | 1-2 |
| Understanding the OPERA Property Management Environment..... | 1-2 |
| Recommended Deployment Configurations | 1-3 |
| Component Security | 1-3 |
| Browser Security | 1-3 |
| Networking Security | 1-3 |
| Oracle Database Security | 1-3 |
| WebLogic Server Security..... | 1-3 |
| 2 Performing a Secure OPERA Property Management Installation..... | 2-1 |
| The 12 Requirements of the PCI DSS | 2-1 |
| Installing OPERA Property Management Securely | 2-2 |
| Post-Installation Configuration..... | 2-3 |
| Setting Up Passwords..... | 2-4 |
| 3 Implementing OPERA Property Management Security | 3-1 |
| OXI..... | 3-1 |
| Setup Configuration | 3-1 |
| Property Configuration..... | 3-1 |
| Utilities | 3-1 |
| Export | 3-2 |
| Global Application Parameters in an ASP Environment..... | 3-2 |
| Permissions..... | 3-2 |
| LDAP Configuration | 3-2 |
| 4 Security Considerations for Developers..... | 4-1 |

Preface

This document provides security reference and guidance for OPERA Property Management.

Audience

This document is intended for:

- OPERA Customers
- Oracle Installers
- Oracle Dealers
- Oracle Customer Service
- Oracle Training Personnel
- MIS 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 and any associated log files
- Screen shots of each step you take

Related Documentation

PCI Security Standards Council Reference Documents

The following documents provide additional detail for the Payment Applications - Data Security Standard (PA-DSS) and related security programs, such as Payment Card Industry Data Security Standard (PCI DSS) and Open Web Application Security Project (OWASP):

- PA-DSS
https://www.pcisecuritystandards.org/security_standards/index.php
- PCI DSS
https://www.pcisecuritystandards.org/security_standards/index.php
- OWASP
<http://www.owasp.org>
- Center for Internet Security (CIS) Benchmarks (used for OSHardening)
<https://benchmarks.cisecurity.org/downloads/multiform/>

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

Revision History

| Date | Description of Change |
|---------------|--|
| June 2018 | <ul style="list-style-type: none">• Initial publication |
| April 2019 | <ul style="list-style-type: none">• Updated for 5.6.5 |
| February 2020 | <ul style="list-style-type: none">• Updated for 5.6.9 |
| October 2020 | <ul style="list-style-type: none">• Updated for 5.6.12 |
| May 2023 | <ul style="list-style-type: none">• Added advisory to OPERA Property Management Network pg. 1-2. |

1 OPERA Property Management Security Overview

This chapter provides an overview of Oracle Hospitality OPERA Property Management security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

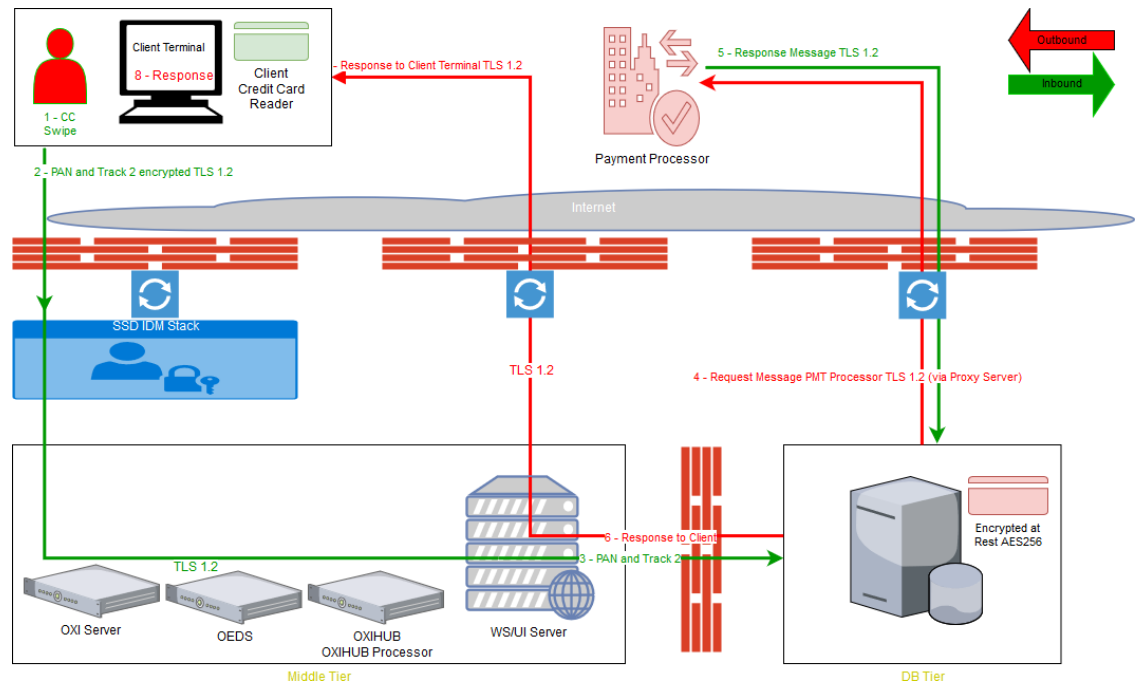
- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. Refer to the *Performing a Secure OPERA Property Management Installation* section in this document for more information.
- **Learn about and use the OPERA Property Management security features.** Refer to the *Implementing OPERA Property Management Security* section in this document for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. Refer to the *Security Considerations for Developers* section in this document for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the *Critical Patch Updates and Security Alerts* website: <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Overview of OPERA Property Management Security

OPERA Property Management Network

The network diagram below shows connection directly through the Internet. However, most deployments use the preferred private network connection configuration.

Never expose or connect your on-premises systems to the internet without strict firewall and security protocols in place such as using reverse proxy.



OPERA Property Management Database Server Components

- Oracle Database 11.2.0.4 or 12.2.1.3
- OEL 6.x or OEL 7.x
- Windows Server 2016

You can use either OEL 6.x/7.x or Windows Server 2016 for hosting the Oracle Database.

Understanding the OPERA Property Management Environment

When planning your OPERA Property Management implementation, consider the following:

- **Which resources need to be protected?**
 - 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. You can 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 strategic resources 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. Understanding the security ramifications of each resource will help you protect it properly.

Oracle provides functionality within the OPERA Property Management 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 PA-DSS rules and regulations.

Recommended Deployment Configurations

For more information, see the *Oracle® Hospitality OPERA Property Management User Guide* and *PA-DSS Implementation Guide* on the Oracle Help Center website at <https://docs.oracle.com/en/industries/hospitality/?tab=2>.

Component Security

Use only HTTPS or Transport Layer Security (TLS) security with a certification authority for the OPERA Property Management application.

Browser Security

For information on browser security, visit <https://us-cert.cisa.gov/publications/securing-your-web-browser>

Networking Security

For information on networking security, visit the Oracle Help Center website at http://docs.oracle.com/cd/B19306_01/network.102/b14266/checklis.htm#i1009371

Oracle Database Security

For the Oracle Database Security Guide 11.2, visit the Oracle Help Center website at <https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dbseg/index.html>

WebLogic Server Security

For the Oracle Fusion Applications Administrator's Guide 11.1.2., visit the Oracle Help Center website at <https://docs.oracle.com/middleware/12212/cross/securedocs.htm>

2 Performing a Secure OPERA Property Management Installation

This chapter presents planning information for your OPERA Property Management installation.

For information about implementing OPERA Property Management, visit the Oracle Help Center website at <http://docs.oracle.com/en/industries/hospitality/?tab=2>.

The 12 Requirements of the PCI DSS

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel.

For more information, see the *Oracle® Hospitality OPERA Property Management User Guide*.

Installing OPERA Property Management Securely

You must review the PA-DSS Implementation Guide and review the following security topics in the OPERA User Guide before installing OPERA Property Management:

- OPERA Property Management Implementation
- Credit Card Encryption Key Utility

To view these guides, visit the Oracle Help Center website at <http://docs.oracle.com/en/industries/hospitality/?tab=2>.

Oracle strongly recommends that all systems containing sensitive information (servers, databases, wireless access points) reside behind a firewall to protect its data.

- * *Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems must be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.*

OPERA Property Management installation media prompts you to change passwords upon installation. You should not use default or well-known passwords and you should frequently rotate your passwords.

Oracle recommends that you secure all sensitive information transmitted over the Internet using a form of encryption such as TLS Protocols; this includes all wireless transmissions, email, and services such as Telnet and SFTP.

Oracle recommends using IPSec between the application and database servers to secure communications. The IPSEC tunnel is also the proposed solution for all other servers that connect directly to the database (OWS, ADS, GDS, OXI).

When using our web-based credit card interface, we suggest configuring it to use TLS1.2 Protocol for communication. To configure this, do the following: Select **Configuration**, then **Setup**, then **Property Interfaces**, and then **Interface Configuration** and edit the active EFT Interface. There is a section on the screen to configure the URL for connecting to the interface. Be sure that the URL starts with HTTPS. This ensures a secure TLS1.2 Protocol connection is made to the vendor prior to transmitting credit card data.

For backend access for third-party systems, you must use the Oracle Service Bus (OSB), and you must not grant direct access to the database.

Post-Installation Configuration

- Remove or disable components that are not needed in a given type of deployment.
- Follow OPERA Property Management installation media prompts to change passwords upon installation.
- Use complex passwords and frequently change them.
- Configure communications security. Only configure secure protocols such as SFTP and HTTPS.
- Use Transport Layer Security (TLS).
- Protect sensitive data: restrict access to Log files under \MICROS\OPERA\LOGS.
- Close Port 1521.
- Secure Export Directories (UNC) from unauthorized access.
- Revoke certain database permissions when manually installing the Database. For more information, see “Oracle Database Security” in the *Oracle® Hospitality OPERA Property Management User Guide*.

Database Permissions that must be revoked:

```
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
REVOKE SELECT ANY TABLE FROM PUBLIC;
REVOKE CREATE ANY TABLE FROM PUBLIC;
REVOKE CREATE ANY DIRECTORY FROM PUBLIC;
REVOKE SELECT ON ALL_USERS FROM PUBLIC;
REVOKE SELECT ON ALL_TAB_PRIVS FROM PUBLIC;
REVOKE SELECT ON ALL_SOURCE FROM PUBLIC;
REVOKE SELECT ON ALL_DB_LINKS FROM PUBLIC;
```

Setting Up Passwords

The OPERA Property Management installation media prompts you to change passwords.

When creating the first property in a Schema, the application prompts and forces the change of the OPERA Supervisor password.

Use Complex Passwords and frequently change those passwords.

Do not grant a regular user access to the OPERA 5 Supervisor Group. This group or members from this group must only be used by authorized Data Center Administrators.

3 Implementing OPERA Property Management Security

If OPERA Property Management is deployed in ASP mode, you must follow the “OPERA ASP Implementation” process as described in the *Oracle® Hospitality OPERA Property Management User Guide*.

When in ASP mode, you should never grant a property user access to certain areas of the application. This includes, but is not limited to, the following:

OXI

- OXI COMMUNICATION METHODS – OXI Communication Methods setup
- OXI DELETE ERROR LOG – OXI DELETE System Error Log
- OXI DELETE INTERFACE – OXI Delete Interface Setup
- OXI LICENSE – OXI License Setup
- OXI START PROCESS – OXI Start / Stop Process
- OXI SYSTEM ERROR LOG – OXI Show System Error Log

Setup Configuration

- BUSINESS EVENTS CONFIGURATION – Business Events Configuration
- BUSINESS EVENTS EXTERNAL SYSTEMS – Business Events External Systems Configuration
- BUSINESS EVENTS QUEUE STATUS – Business Queue Status Configuration
- SCREEN DESIGN – Screen Painter
- SCREEN PAINTER UNDOALL – Screen Painter Undo All Changes

Property Configuration

- PROPERTY NEW – Create New Properties

Utilities

- The complete UTILITIES Permission group

Export

- BACK OFFICE – Back Office Configuration
- COUNTRY EXPORTS – Country Export Configuration
- EXPORT FILE – Export Files Configuration
- SALES CATERING – Sales and Catering Configuration
- EXTERNAL SC EXPORT – External SC Export Configuration
- MEMBERSHIP EXPORT – Membership Export Configuration

Global Application Parameters in an ASP Environment

All Global application parameters should have the DISPLAY_YN flag in the application_parameters table set to N.

Permissions

- Do not grant access by any user to the OPERA SUPERVISOR and OPERA Supervisor groups. These accounts are reserved for authorized Data Center Administrators only.
- Do not give the OPERA Supervisor password to any user.
- Grant the CREDIT CARD INFORMATION EDIT permission to users only as needed.

You should configure users with the least amount of privileges/permissions.

By default, the system sets User Login and Password change and Password complexity parameters to a secure level.

You should regularly check Security Advisories on the Oracle website.

- Implement security fixes in a timely manner.
- Apply the latest certified CPU updates.

LDAP Configuration

The User on the LDAP System screen (select Configuration, Setup, LDAP Configuration, and then New) must be a low level LDAP user and must not be a user in OPERA or have any OPERA roles assigned. This User is only needed for the LDAP Cleanup function. For more information, refer to the *OPERA Property Management User Guide* on the Oracle Help Center website at <http://docs.oracle.com/en/industries/hospitality/?tab=2>.

4 Security Considerations for Developers

The following security checklist includes 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.

To learn how to secure OPERA Property Management and its components, you must review the *OPERA Property Management User Guide* and *PA-DSS Implementation Guide* on the Oracle Help Center website at <http://docs.oracle.com/en/industries/hospitality/?tab=2>