Oracle® Hospitality OPERA Property Management

Security Guide

Versions: 5.0.05.00

Part Number: E67891-01

May 2016

ORACLE®

Contents

Preface

Audience

- OPERA Customers
- Oracle Installers
- Oracle Dealers
- Oracle Customer Service
- Oracle Training Personnel
- MIS Personnel

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 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
01-Oct-2015	Initial publication.
13-May-2016	LDAP Configuration

Chapter 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

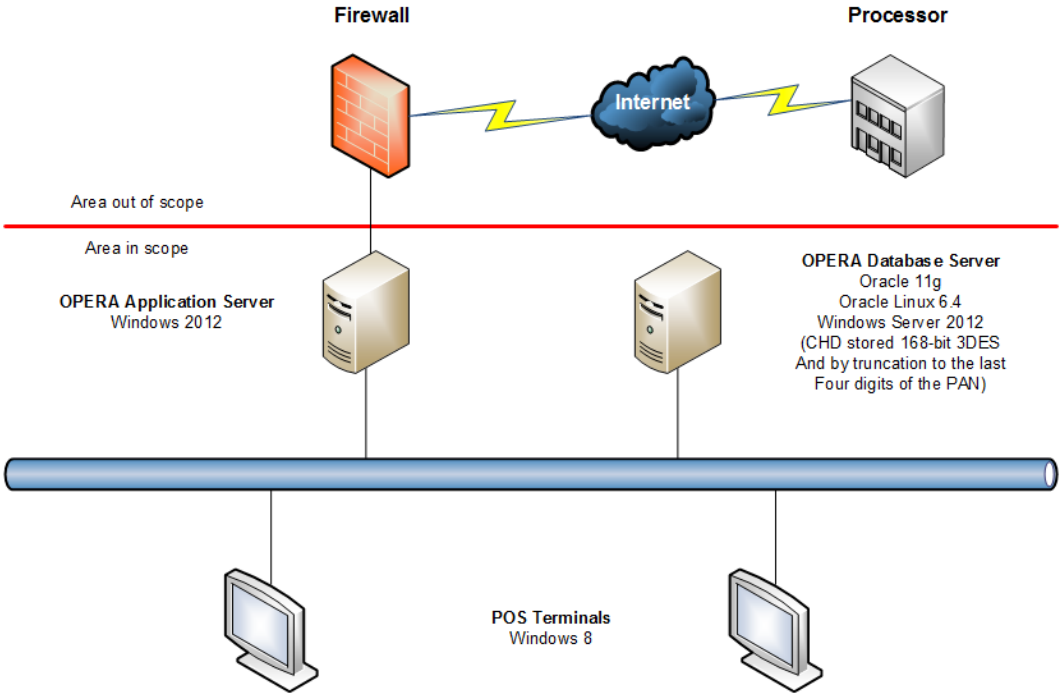
The following principles are fundamental to using any application securely:

- **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. Organizations should review user privileges 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 Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) and secure passwords. For more information, see Chapter 2.
- **Learn about and use the OPERA Property Management security features.** For more information, see Chapter 3.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
- **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. For more information, visit the Oracle Critical Patch Updates and Security Alerts website at 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.



OPERA Property Management Database Server Components

- Oracle 11gR2
- Oracle Linux 6.x
- Windows Server 2012r2

You can use either Oracle Linux 6.x or Windows Server 2012r2 for hosting the Oracle 11gR2 Database.

Understanding the OPERA Property Management Environment

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

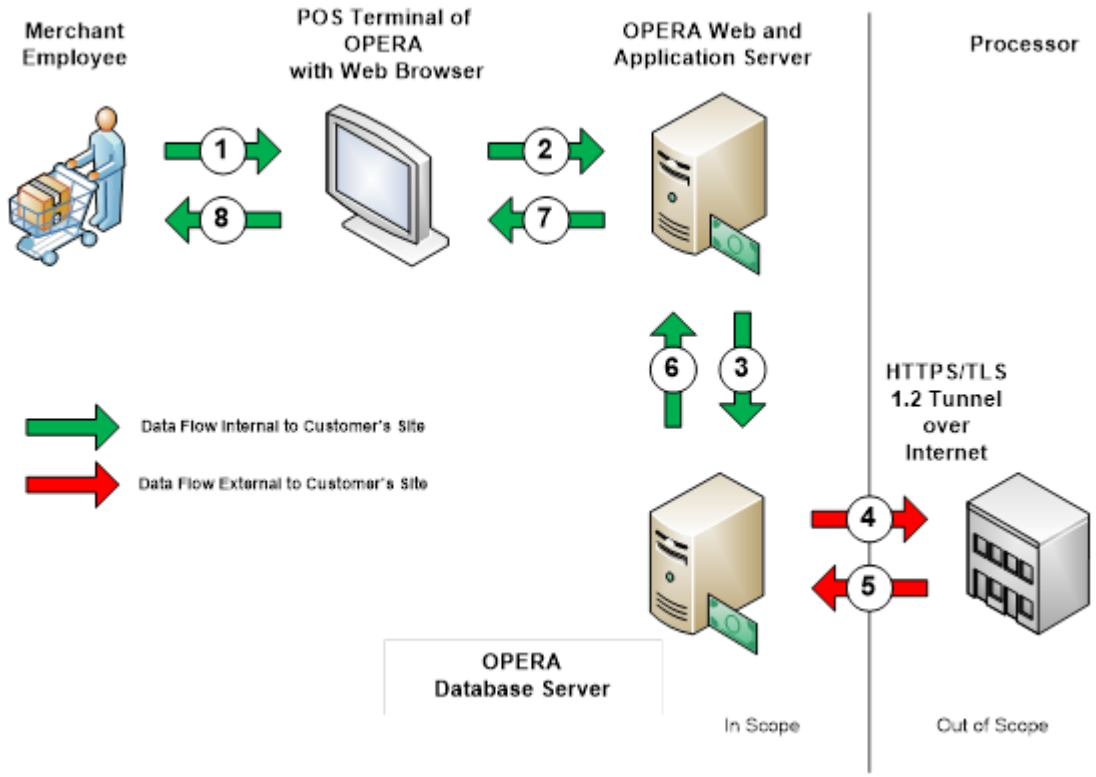
- **Which resources need protection?**
    - You need to protect customer data, such as credit-card numbers.
    - You need to protect internal data, such as proprietary source code.
    - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers or tenants (ASP mode), but someone in your organization (Data Center Administrators) 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 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. 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

This section describes recommended deployment configurations for OPERA Property Management.

Credit/Debit Cardholder Dataflow



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

OPERA Property Management Component Security

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

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 http://docs.oracle.com/cd/E25054_01/network.1111/e16543/toc.htm

WebLogic Server Security

For the *Oracle Fusion Applications Administrator's Guide 11.1.2.*, visit the Oracle Help Center website at http://docs.oracle.com/cd/E25054_01/fusionapps.1111/e14496/securing.htm

Chapter 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 https://docs.oracle.com/cd/E53533_01/index.html

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 *Oracle® Hospitality OPERA Property Management Implementation Guide*.

Installing OPERA Property Management Securely

You must review the following security topics in the OPERA User Guide before installing OPERA Property Management:

- OPERA Property Management Implementation
- Credit Card Encryption Key Utility
- Configuring OPERA for SSL Communication
- IPsec Configuration
- Changing Passwords in an OPERA System
- OPERA ASP Implementation

To view the OPERA User Guide, visit the Oracle Help Center website at https://docs.oracle.com/cd/E53533_01/index.html#

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). For more information on the configuration of this feature, see *IPsec Configuration*.

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 > Setup > Property Interfaces > 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 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.

Chapter 3: Implementing OPERA Property Management Security

If OPERA Property Management is deployed in ASP mode, you must follow the *OPERA ASP Implementation 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 CONFIG

- 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 CONFIG

- 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, see the OPERA Property Management User Guide on the Oracle Help Center website at http://docs.oracle.com/en/industries/hospitality/?tab=2.

Appendix A: Secure Deployment Checklist

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.

      ii. Revoke unnecessary privileges from the PUBLIC user group.
      iii. 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.

You must review the following security topics in the OPERA User Guide before installing OPERA Property Management:

- OPERA Property Management Implementation
- Credit Card Encryption Key Utility
- Configuring OPERA for SSL Communication
- IPsec Configuration
- Changing Passwords in an OPERA System
- OPERA ASP Implementation

To view the OPERA User Guide, visit the Oracle Help Center website at https://docs.oracle.com/cd/E53533_01/index.html#