Oracle® Hospitality Hotel Property Interface

Security Guide
Release 8.15.3.0
Part Number: F58398-02

July 2023

ORACLE

1 Contents

Preface

This document provides security reference and guidance for Oracle Hospitality Hotel Property Interface.

Audience

This document is intended for:

- System administrators installing Oracle Hospitality Hotel Property Interface.
- End users of Suite8 or OPERA Hotel Property Interface.

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
- 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/

Related Documentation

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, and so forth.):

- Payment Card Industry - Security Standard – Document library (e.g. PCI DSS and PCI PA-DSS)
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)

Guides and Best Practices:

- *Oracle Hospitality Hotel Property Interface Installation Guide, version 8.15.0*
- *Oracle Hospitality Suite8 Security Guide*
- *Oracle Hospitality OPERA Property Management Security Guide*
- *Oracle Hospitality OPERA Cloud Services Security Guide*
- *Oracle Hospitality Suite8 Property PA-DSS Data Security Standard Implementation Guide, Version 8.10.1*

Revision History

Date	Description of Change
March 2019	• Initial publication.
September 2021	• Bi-Annual Review for compliance current version 8.14.12.0
May 2022	• Bi-Annual Review for compliance current version 8.15.0.0
October 2022	• Bi-Annual Review for compliance current version 8.15.1.0 • Updated links
June 2023	• Bi-Annual Review for compliance current version 8.15.3.0 • Added section 'Securing communication (TLS/SSL)'

1 Hotel Property Interface Security Overview

This chapter provides an overview of Oracle Hospitality Hotel Property Interface security and explains the general principles of application security when installing with Oracle Hospitality Suite8 Property Management or with Oracle Hospitality OPERA Property Management.

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. See "Performing a Secure Hotel Property Interface Installation" for more information.
- **Learn about and use the Hotel Property Management security features.** See "Implementing Suite8 Property Management Security" for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See "Security Considerations for Developers" 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 Web site:

Overview of Hotel Property Interface Security

In accordance with the PA-DSS (Data Security Standard), Oracle strongly recommends that every site installs and maintains a firewall configuration to protect data. Configure your network so that databases and client PCs always reside behind a firewall and have no direct access to the Internet.

Oracle strongly recommends that each site ensures that servers, databases, client PCs, and any medium containing sensitive data reside behind a firewall.

Firewalls are computer devices that control the 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 need to 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.

Understanding the Suite8 / OPERA Hotel Property Interface Environment

When planning your Suite8 or OPERA Hotel Property Interface implementation, consider the following:

- **Resources that 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 access data to third party interfaces from misuse.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Protecting your data**.

  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.
- **Taking precautions if the 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 Suite8 or OPERA application for Personal Information (for example, passport, date of birth, and credit card). Placing this information in any fields other than the designated areas, for example, Notes or Comments fields, is open for PCI review and is not compliant with PA-DSS rules and regulations.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Suite8.

There are different deployment scenarios possible depending on the used dataflow and installed interfaces.

Credit/Debit Cardholder Dataflow Diagram

The following pictures show examples of the deployment diagram with Electronic Funds Transfer (EFT) vendor connected:

Figure 1-1 Suite8 Property Network Diagram with Credit Card Interface, EFT vendor application located on Premise

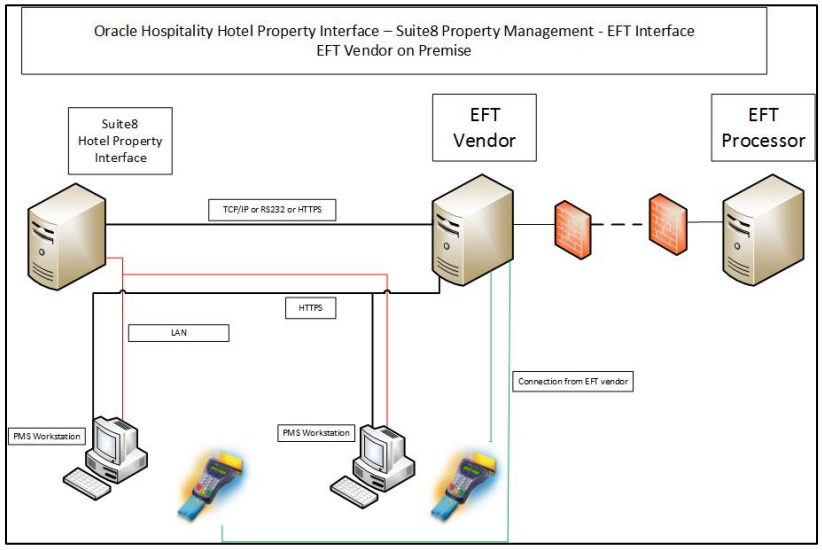


Figure 1-2 Suite8 Property Network Diagram with Credit Card Interface, EFT vendor not located on Premise

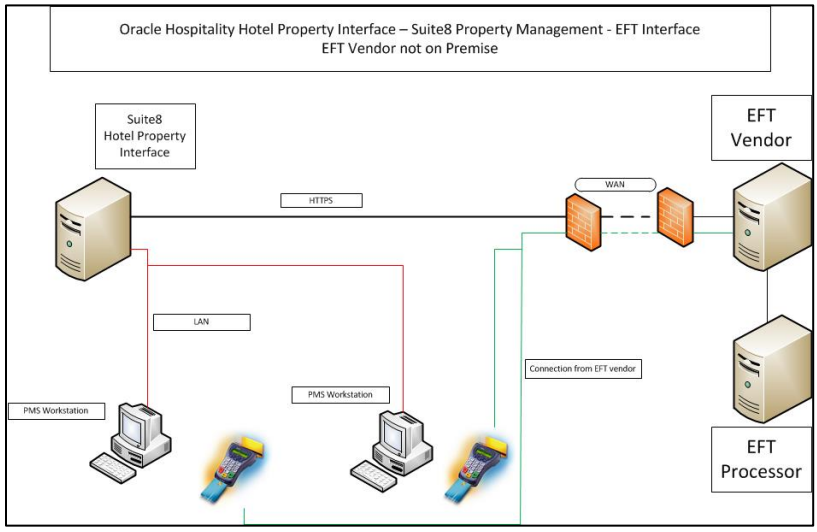


Figure 1-3 OPERA Property Network Diagram with Credit Card Interface, EFT vendor located on Premise

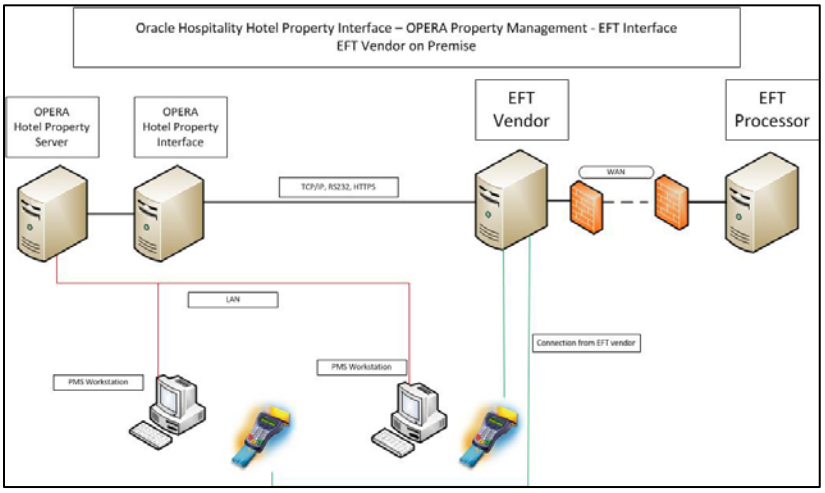
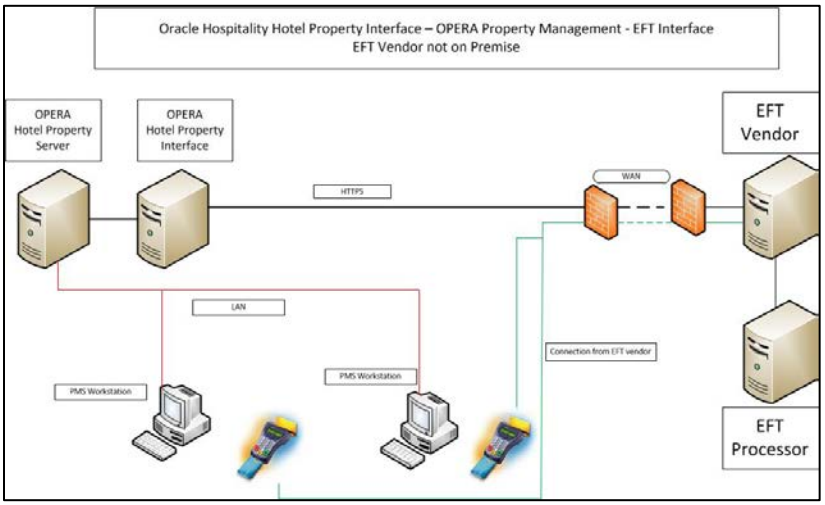


Figure 1-4 OPERA Property Network Diagram with Credit Card Interface, EFT vendor not located on Premise

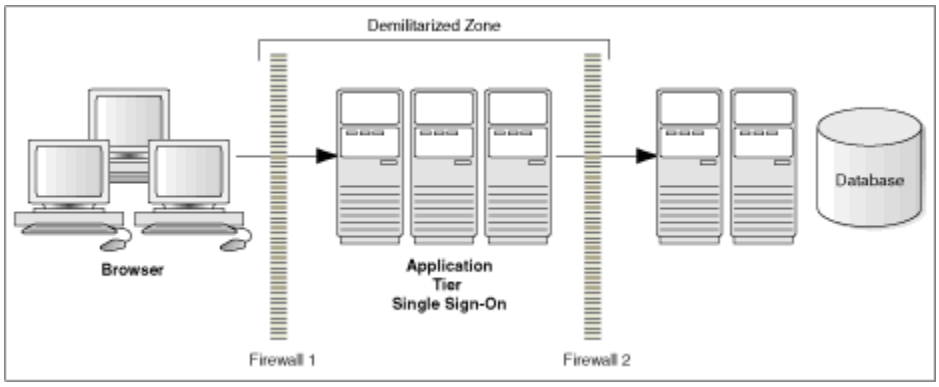


Oracle suggests using Data encryption method for connections between Interface application and vendor system using the Oracle Hotel Property Interface.

With this encryption method the sensitive data based on PA-DSS will be encrypted.

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 1-8.

Figure 1-5 Traditional DMZ View



The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors

Component Security

Operating System Security

See the Network Security Checklists.

Oracle Database Security

See the Oracle Database Security Guide

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

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

Maintain a policy that addresses information security for all personnel. Refer to the latest *Oracle Hospitality Suite8 Property PA-DSS Implementation Guide*. This chapter presents planning information for your Suite8 installation.

For information about installing Suite8, refer to the *Oracle Hospitality* Suite8 *Installation Guide*.

2 Performing a Secure Hotel Property Interface Installation

This chapter presents planning information for your Hotel Property Interface installation. For information about installing Hotel Property Interface, see *the Oracle Hospitality Hotel Property Interface Installation Guide*.

Pre-Installation Configuration

Install and maintain a firewall configuration to protect data.

Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined through public information.

Suite 8 or OPERA do not provide default accounts.

Installing Hotel Property Interface Securely

The following guides are a pre-requisite before installing PMS:

- *Oracle Hospitality Hotel Property Interface Installation Guide, version 8.15.x*
- *Oracle Hospitality Suite8 Property PA-DSS Implementation Guide, Version 8.10.1*

When installing the database, you must create secure database passwords. Do not use default or well-known passwords and rotate passwords frequently.

Post-Installation Configuration

- Remove or disable components that are not needed in a given type of deployment.
- Configure communications security. Weak or plain-text protocols must be disabled. It is still possible to enable them for backward compatibility (or communication with third parties which still don't support secure protocols), however this might be insecure. It is planned for the future versions to completely disable insecure protocols.
- Enable User Access Control.
- Change the User Access Rights for the Oracle Client/Suite8 Client and IFC files to be restrictive (See Suite8 Install Shield_813 for the details).

Configuring Passwords

The Hotel Property Interface application is not installed with any default passwords.
Suite8 PMS:
To run properly, the IFC8 application needs related Oracle Client User and Password being entered in its configuration part. The related password is encrypted once entered and is not visible anymore afterwards.
Ensure that Oracle Client passwords changes are also done within the IFC8 application in related configuration section.

Securing Communication (SSL/TLS)

We strongly recommend using TLS for all communication channels (Vendor / PMS / IfcControl / IfcBusi).

Exact configuration please refer to the configuration document:

- *IFC8 configuration*
- *Review the Cipher Suites in use as to relevance or if obsolete please see https://learn.microsoft.com/en-us/windows-server/security/tls/manage-tls*

3 Implementing Hotel Property Interface Security

Please refer to the following Property Management Security Guides:

- *Oracle Hospitality Suite8 Property Management Security Guide*
- *Oracle Hospitality OPERA Property Management Security Guide*
- *Oracle Hospitality OPERA Cloud Services Security Guide*

Appendix A Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- 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.