Oracle® Hospitality OPERA Cloud Services

Security Guide
Release 1.20
E69079-01

June 2016

ORACLE

Contents

Preface

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

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
- 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 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
08-Feb-2016	Initial publication.

1 OPERA Cloud Security Overview

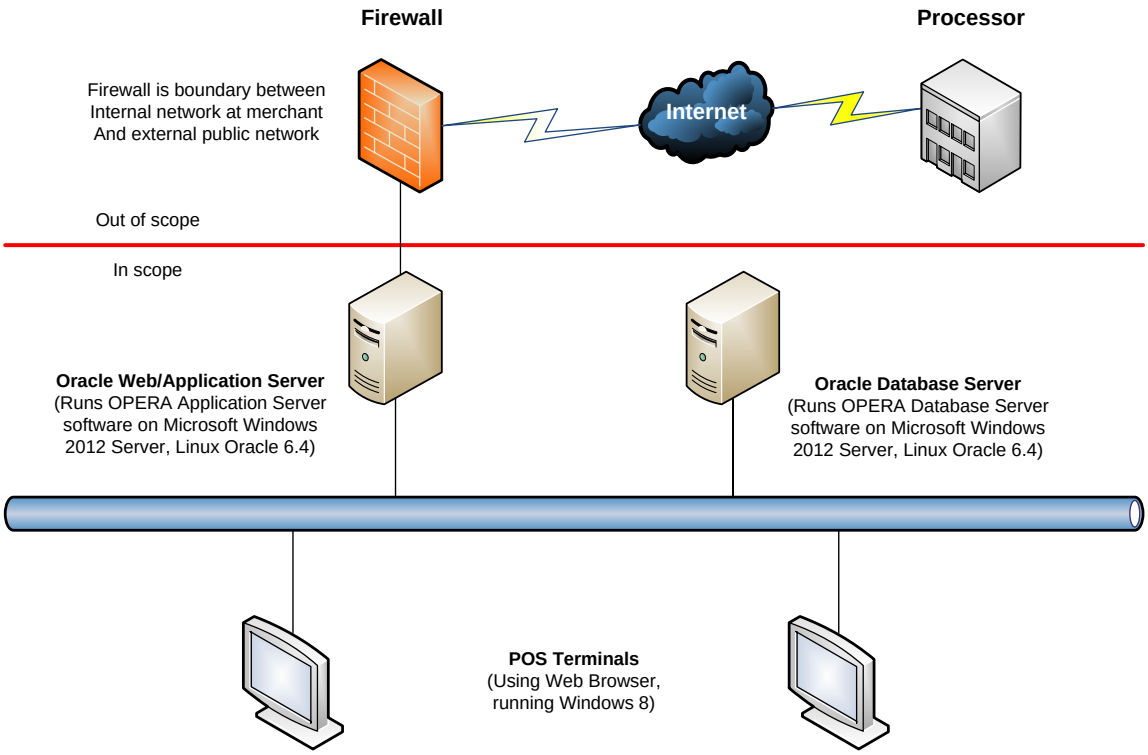
This chapter provides an overview of Oracle Hospitality OPERA Cloud Services (OPERA Cloud) security and explains the general principles of application security.

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 Cloud 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

2 OPERA Cloud Network



OPERA Cloud Server Components

- Oracle Linux 6.4
- Windows Server 2012

3 Understanding the OPERA Cloud Environment

When planning your OPERA Cloud implementation, consider the following:

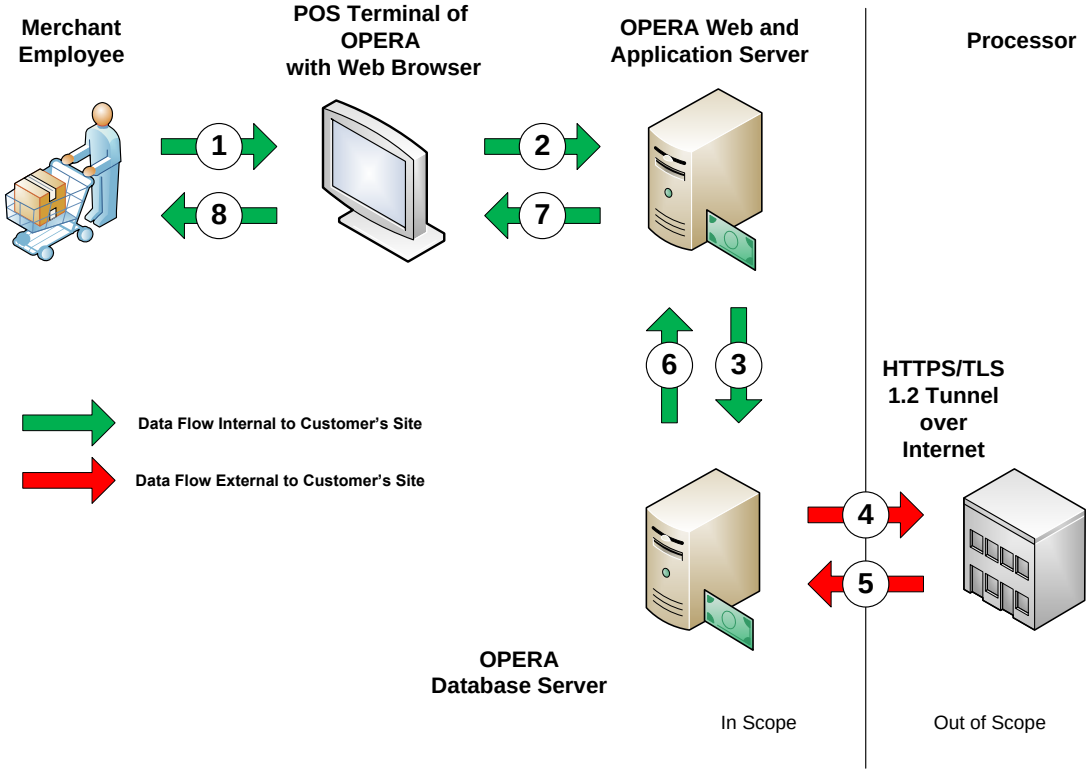
- **Which resources need protection?**
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. 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. Understand the security ramifications of each resource and protect it properly.

Oracle provides functionality within the OPERA 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.

4 Recommended Deployment Configurations

This section describes recommended deployment configurations for OPERA Cloud.

Credit/Debit Cardholder Dataflow



1. Merchant Employee swipes card data on POS terminal or enters card data manually (when card is not present) into the POS terminal.
2. If merchant employee swipes the card, the POS Terminal sends PAN and Track 2 encrypted data to the OPERA Application Server.
3. The OPERA Application Server sends this data to the OPERA Database Server.
4. The OPERA Database formats the data into a request message and sends the transaction to the Processor.

5. The Processor responds with the approval or decline of the transaction.
6. The OPERA Database sends the response to the OPERA Application Server.
7. The OPERA Application Server directs the response to the correct terminal.
8. The terminal displays the response to the user to action if needed or to complete the business transaction.

For more information, see *Oracle® Hospitality OPERA Cloud Services PA-DSS Implementation Guide*.

5 OPERA Cloud Component Security

Use only HTTPS or Transport Layer Security (TLS) security with a certification authority for the OPERA Cloud application.
Use IPsec network protocol to encrypt network traffic. For more information about this protocol, see *IPsec Configuration*.

Operating System Security

For more information on operating system security, see the following documents:

- *Guide to the Secure Configuration of Red Hat Enterprise Linux 5*
- *Hardening Tips for the Red Hat Enterprise Linux 5*

Oracle Database Security

See *Oracle Database Security Guide*.

WebLogic Server Security

See *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

6 Performing a Secure OPERA Cloud Installation

This chapter presents planning information for your OPERA Cloud installation.

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

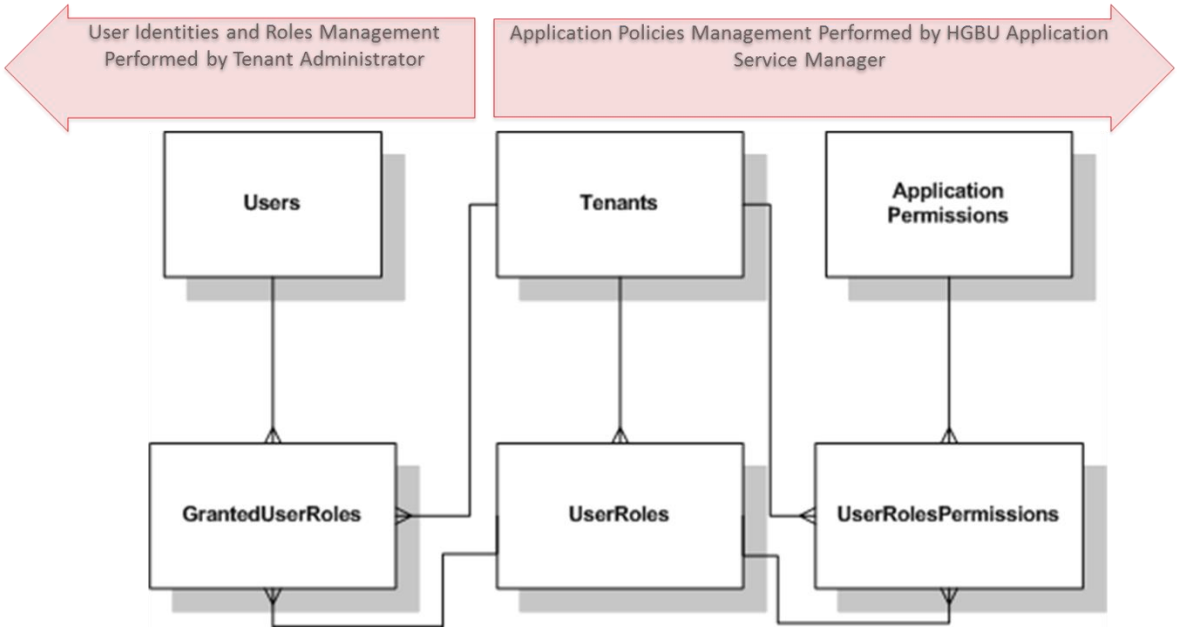
12. Maintain a policy that addresses information security for all personnel.

For more information, see *Oracle® Hospitality OPERA Cloud Services PA-DSS Implementation Guide*.

7 Implementing OPERA Cloud Security

The diagram below shows the management duties performed by the Tenant Administrator and the HGBU Application Service Manager.

Multi-tenant Identity Store Model



The table below lists the user roles, role owners and LDAP privileges of these roles in OPERA Cloud.

User Management – Roles & Privileges

Role	Role Owner	LDAP Privilege			
		Read	Read, Write	Scope	use cases performed
ApplicationAdministrator	Oracle HGBU Cloud Hotel Application Team	X	X	Search base for viewing all users that can access application	Creation of INIT roles. WebLogic and OAM service accounts have this role as well.
<tenantN_code>-INIT	Oracle HGBU OPERA9 Application Manager		X	OU=OPERA and user groups that are prefixed with <tenant1_code>- only	Creates <tenant>SystemAdministrator roles. Creates initial tenant users and grants SystemAdministrator roles to these users.
ApplicationPolicyAccessor	Oracle HGBU Cloud Hotel Application Team		X	OU=OPERA Realm designated for OPERA roles	Back end role which provides other administrative roles with read/write permissions in LDAP. Users of the OPERA Role Manager Application have this role.
<tenant1_code>-SystemAdministrator	Tenant1		X	OU=OPERA and user groups that are prefixed with <tenant1_code>	Administrators of Tenant1. Creates new roles and maps application permissions to roles. Creates new users and grants roles to users. Administration is restricted to Tenant1 and is enforced by the OPERA9 Role Manager application.
<tenant1_code>-Res_Mgr; <tenant1_code>-FrontDesk; ...	<tenant1_code>-SystemsAdministrator role				All application business roles.
<tenantN_code>-SystemAdministrator	TenantN		X	OU=OPERA and user groups that are prefixed with <tenantN_code>	Administrators of TenantN. Same use case as <tenant1_code>-SystemAdministrator.

Appendix A: Secure Deployment Checklist

The following security checklist provides 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.

For more information, see *Oracle® Hospitality OPERA Cloud Services PA-DSS Implementation Guide*.