Oracle® Hospitality eCommerce Integration Cloud Service

Security Guide
Release 18.1
E68585-02

May 2018

ORACLE

Contents

Preface

This document provides security reference and guidance for eCommerce Integration Cloud Service.

Audience

This document is intended for:

- System administrators installing eCommerce Integration Cloud Service.
- End users of eCommerce Integration Cloud Service.

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

Documentation

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

Revision History

Date	Description of Change
March 2018	• Initial publication
May 2018	• Updated Chapters 1 and 2

1 eCommerce Integration Cloud Service Security Overview

This chapter provides an overview of Oracle Hospitality eCommerce Integration Cloud Service security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

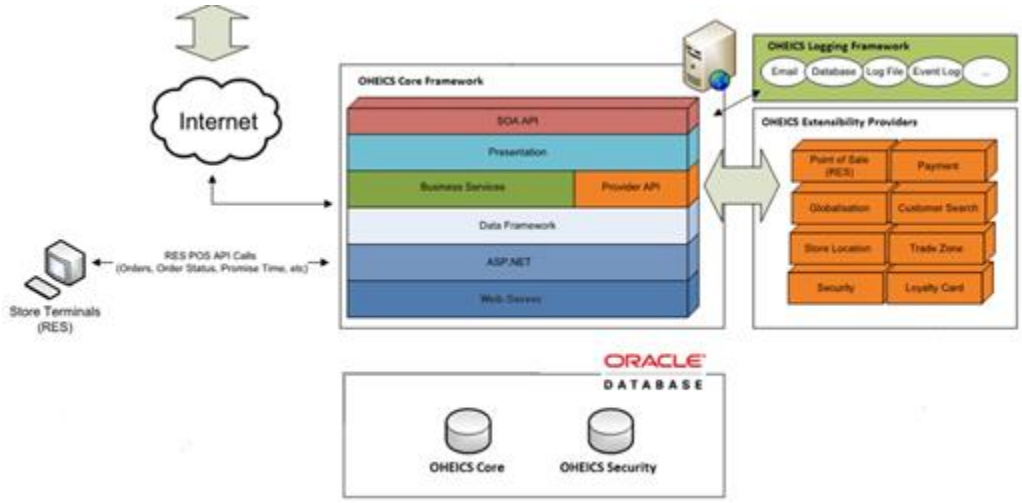
- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Learn about and use the eCommerce Integration Cloud Service security features.** See Implementing eCommerce Integration Cloud Service Security 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.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.

Overview of eCommerce Integration Cloud Service Security

The Oracle Hospitality eCommerce Integration Cloud Service contains several components deployed in the Oracle Hospitality Cloud.

The application contains the main ordering application that communicates with the Oracle Database. The application runs through a web server to expose several web services that interact with client applications.

PA-DSS validated applications should reference the application's *PA-DSS 3.1 Implementation Guide*, specifically Chapter 2: Executive Summary, sections including the "Typical Network Implementation" and the "Credit/Debit Cardholder Dataflow Diagram" to complete this section.



2 Implementing eCommerce Integration Cloud Service Security

This chapter explains implementation of the Oracle Hospitality eCommerce Integration Cloud Service security features and how to maintain a secure environment.

To keep the application secure, you must:

- Follow Oracle Database security recommendations
- Create and update user names and passwords
- Maintain automatic credit card key encryption
- Delete customer data
- Assign and manage Roles and Privileges
- Monitor user's activities in the Audit Log

Data Encryption

Data is transmitted via HTTPS and TLS 1.2 encryption is used by default for secure data communication.

The database is encrypted using Transparent Data Encryption on all tablespaces. For more information about Transparent Data Encryption see https://docs.oracle.com/database/121/ASOAG/asopart1.htm#ASOAG600.

Database Security

See the Oracle Database Security Guide (located at https://docs.oracle.com/database/121/ASOAG/toc.htm) for more information about Oracle Database security.

Automatic Key Encryption

By default, the application uses automatic key encryption. Automatic key encryption rotates the encryption key each time the credit card data is encrypted. When the credit card encryption is requested, a new encryption key automatically generates to encrypt the data. After encryption is complete, the encryption key is not persisted anywhere and another new key generates when the next credit card data encryption request is received. In this way, the encryption key is automatically rotated with every new credit card data encryption request. The key is never stored in the database or on the hard disk, and there is no need for manual key rotation. As another layer of security, the encryption key is encrypted as well.

Delete Historical Data

The application never stores magnetic stripe data, card validation codes, PINs, or PIN blocks.

Prior to using version 18.1, you must remove stored encrypted history using the purge utility in the System Administration Tools section of the application.

To instantly delete historical data:

1. Go to the System Administration **Tools**.
2. In the **Client** section, click the **Clear ClientPassword** button.

Purge Cardholder Data

You must purge cardholder data exceeding the merchant-defined retention period. To accomplish this function you must request hosting to schedule a purge job.

Scheduling a Purge Job on the Oracle 12c Database Server

If more than one database requires purging, you must schedule a purge job for each database.

1. Connect to the User Schema that requires purging of data.
2. Go to the **Scheduler** section and open the **Jobs** folder.
3. Select the **Purge Payments** job and name the task accordingly.
4. Schedule a job using the job window in the Job Details tab, and select **When to Execute Job**.

Purging Cardholder Data Manually

This option purges cardholder data for all customers.

1. Log in as the System Administrator and access the System Administration **Tools**.
2. Navigate to the **Purge Payments** section, and then select **Purge** to delete the data.

Audit

The Audit log uses a database table and log files to capture all activities for the current user, including making changes in the administration tools and tracking access to personal information (PI). All changes, additions, and deletions made in the administration tools are audited. Accessing, exporting, and changing PI is captured in the audit log.

Users can view each action taken on the PI record, when it was updated, who made the changes, the action performed, and a description of the action.

Using the Audit Trail Tracking Tool

You can view system users and their actions using the Audit Trial Log. Follow the steps in the *Oracle Hospitality eCommerce Integration Cloud Service Configuration Guide* (Managing Roles and Privileges section) to assign Audit Trail privileges to a role. Assign Audit Trail privileges to the user with the client administrator role assigned on brand level only.

Audit Trail Privileges

- **View_EventLog_AuditTrail**: Ability to search and view the Audit Trail tracking.
- **Purge_EventLog_AuditTrail**: Ability to delete Audit Trail entries.

Searching for User Actions

When you use the Audit Trail Search feature with no filters applied, all users and all system activity results appear.

The Audit Trail filters allow you to search using one or a combination of these options:

- Specific system user's actions
- Description of the change
- Module where a change occurred
- Starting date and ending date range

Purging the Audit Trail

You can purge the audit trail if you have the **Purge_EventLog_AuditTrail** privilege.

Follow these steps:

1. In the System Administration **Tools**, navigate to **Audit Trail Search**.
2. Click the **Purge** tab.
3. Select the date from **Purge Records Before**, and then click **Purge**. A Purge Successful confirmation message will appear.

Logging

All Oracle Hospitality eCommerce Integration Cloud Service logs include the timestamp, current level, message level, zone, and thread Id. By default, application logs do not contain PI. Controllers do not have access to the application logs or to configuration. Oracle Support can provide logs upon request.

By default, the log level is set to 0 (no PI logged). If the log level exceeds 2, the PI is logged. This configuration can be changed only for debugging purposes. After debugging, change the log level configuration back to 0.

To provide application logs where PI is captured:

1. Navigate to the UISServices log location and locate **LogZone_UISupportSer.txt**.
2. Edit the file, which contains three lines represented by a number. The numbers correspond to these items in the following order:
    a. Number of logging zones
    b. Name of zone
    c. Log level
3. Change the Log level to 2 and save the file.

Log Retention

File system logs are retained for 90 days by default. The number of days is configurable in the web.config file of UISupportService and Tools.

The application automatically deletes log files that are older than the configured number of days.

web.config configuration:

<add key="MaxLogRetentionDays" value="90"/>

Appendix A Secure Deployment Checklist

This appendix lists actions you must perform to deploy a secure system.

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.