Oracle® Hospitality Cruise Fine Dining System

Security Guide
Release 9.0.2.29
E99054-01

August 2018

ORACLE

Copyright © 2015, 2018, 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 **2**
Audience 2
Customer Support 2
Documentation 2
Revision History 2
1 Fine Dining System Security Overview **3**
Basic Security Considerations 3
Overview of Fine Dining System Security 3
Fine Dining System Architecture Overview 3
Technology 3
User Authentication 4
Understanding the Fine Dining System Environment 4
Recommended Deployment Configurations 5
Component Security 6
Operating System Security 6
Oracle Database Security 6
2 Performing a Secure Fine Dining System Installation **7**
Pre-Installation Configuration 7
Fine Dining System Installation 7
Post-Installation Configuration 7
Operating System 7
Application 8
Passwords Overview 8

Preface

This document provides security reference and guidance for Fine Dining System.

Audience

This document is intended for:

- System administrators installing Fine Dining System.
- End users of Fine Dining System.

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
August 2018	• Initial publication

1 Fine Dining System Security Overview

This chapter provides an overview of Oracle Hospitality Fine Dining System 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 Transport Layer Security (TLS) (SSL), and secure passwords. *See Chapter 2 Performing a Secure Fine Dining System Installation* for more information.
- **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. See the “Critical Patch Updates and Security Alerts” website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Fine Dining System Security

Fine Dining System Architecture Overview

Fine Dining System uses N-Tier Architecture and is a collection of applications and interfaces. It is scalable and do not have to be deployed on a single machine.

Technology

Fine Dining System product is developed using industry standards of encryption. Every communication can be configured to use TLS if required. It also uses powerful encryption/hashing algorithms (Microsoft Windows Data Protection Application Programming Interface (DPAPI), Password-Based Key Derivation Function 2 (PBKDF2)) to encrypt and store sensitive information like application user passwords, application configuration information and database user passwords.

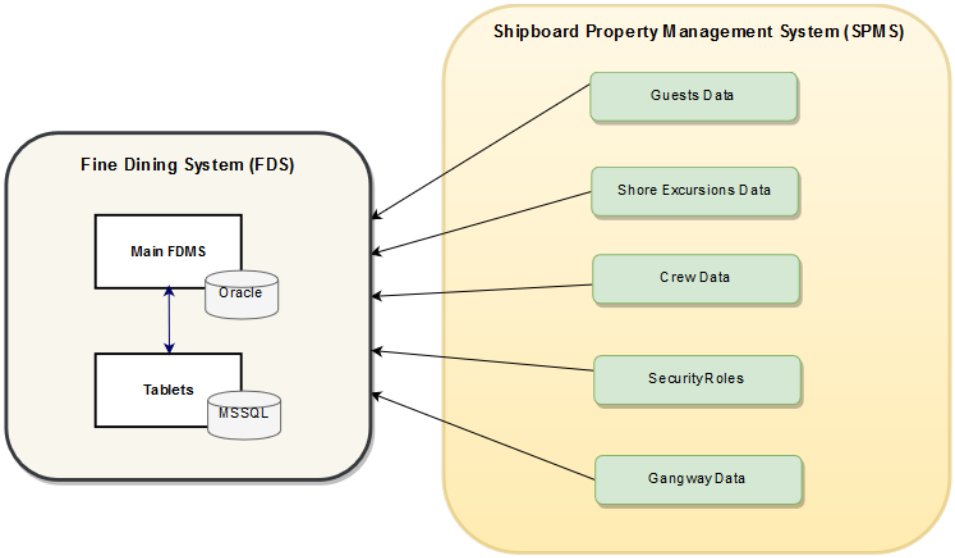

Figure 1 – Fine Dining System Architecture

User Authentication

Overview

Authentication is the process of ensuring that people are who they say they are.

Client Authentication

All users' credentials of Fine Dining System are stored in the database. Anyone who wish to access the clients must provide a valid user name and password. To ensure strict access control of the Fine Dining System, always assign unique usernames and complex passwords to each user. Password must be at least 8 characters long including letters and numbers.

Database Users

Fine Dining System works with both Oracle Server databases.

Understanding the Fine Dining System Environment

When planning your Fine Dining System implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data.
  - 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.

Recommended Deployment Configurations

This section describes the recommended deployment configurations for Fine Dining System.
The Fine Dining System product can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in Figure 2 - Single-Computer Deployment Architecture.

This single-computer deployment may be cost effective for small organizations; however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

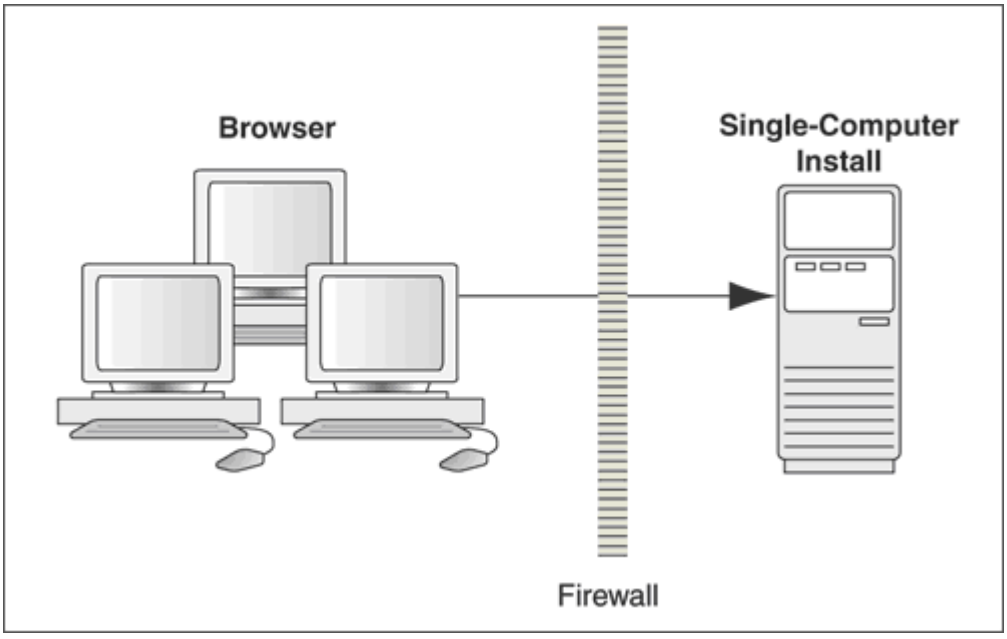

Figure 2 - Single-Computer Deployment Architecture.

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 3 - Traditional DMZ View.

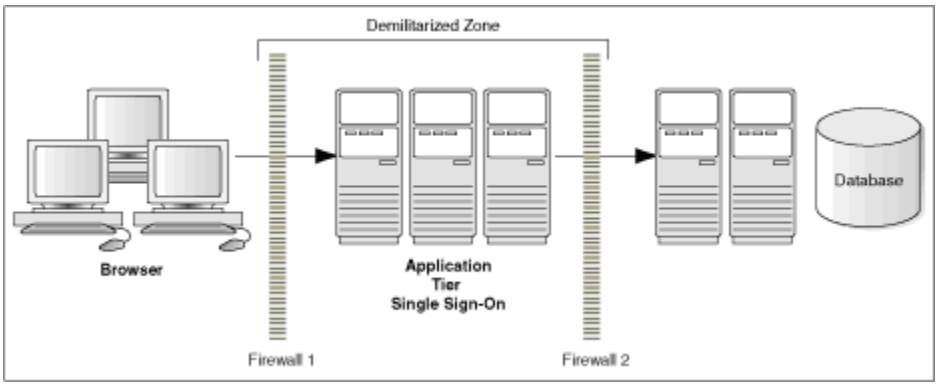

Figure 3 - Traditional DMZ View

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 provides 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

Prior to installation of Fine Dining System, it is essential that the operating system are updated with the latest security updates.
Refer to the following Microsoft TechNet articles for more information about operating system security:

- Windows Server 2012 Security
- Windows Server 2008 R2 Security

Oracle Database Security

Oracle Database

Refer to the Oracle Database Security Guide for more information about Oracle Database security.

2 Performing a Secure Fine Dining System Installation

This chapter presents planning information for your Fine Dining System installation.

Pre-Installation Configuration

Prior to installation of Fine Dining System, perform the following tasks:

- Apply critical security patches to the operating system
- Apply critical security patches to the database server application
- Acquire TLS compliant security certificate from Certification Authority

Fine Dining System Installation

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation. The installation requires the user running the installation to have an administrator privileges. No other users have the required access to successfully complete the installation.
When creating a database, enter a complex password that adheres to the database hardening guides for all users.

The following modules are required for proper operation of the system:

DMS Web Service Helper
DMS Database Installer
DMS Display
DMS System
DMS Web Service
DMS Mobile Client
DMS Mobile Service
DMS Mobile Updater Service

Post-Installation Configuration

This section explains the additional security configuration steps to complete after Fine Dining System is installed.

Operating System

Turn On Data Execution Prevention (DEP)

Turn on DEP if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Auto Play

Turn off Auto play if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Remote Assistance

Turn off Remote Assistance if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Application

Software Patches

Apply the latest Fine Dining System patches available on My Oracle Support, if any. Follow the deployment instructions included with the patch.

Passwords Overview

The configuration of Fine Dining System product passwords is performed in the Fine Dining System Administration module. Administrators are recommended to configure a strong password policy after initial installation of the application and review the policy periodically.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

1. The password must be at least 8 (eight) characters long.
2. The password must contain letters, numbers.
3. Must not choose a password equal to the last 3 (three) passwords used.

Change Default Passwords

Fine Dining System is installed with a default administrative user and password. Please change the default administrative user password in the Fine Dining System, following the above guidelines, after logging in for the first time.

Configure User Accounts and Privileges

When setting up users of the Fine Dining System application, ensure that they are assigned the minimum privilege level required to perform their job function. User privileges are described in Access Control of the user guide.