Oracle® Hospitality Suite8

Security Guide

Release 8.12.0 and higher
F44203-01
June 2021

Oracle Hospitality Suite8 Security Guide Release 8.12.0 and higher

F44203-01

Contents

Preface

This document provides the security reference and guidance for Suite8

Audience

This document is intended for:

1. System administrators installing the Suite8 application
2. End Users of the Suite8

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

Documentation

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

Revision History

Date	Description of Change
December 2020	• First draft of Security Guide
June 2021	• Formatted and edited the guide for Oracle styles and standards

1

Suite8 Security Overview

This guide provides an overview of Oracle Hospitality Suite8 security and explains the general principles of security application.

Basic Security Considerations

The following principles are fundamentals 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 must be given the access necessary only 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.
- **Learn about and use the Suite8 security features**: See Implementing Suite8 for more information about application security features.
- **Use secure development practices:** Take advantage of existing database platform 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* at: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
- **Testing:** Testing is performed regularly with Suite8 along with the latest Oracle and Microsoft software patches.

Overview of the Suite8 Security

Suite8 as a product uses the three layer architecture-

1. Windows forms the UI layer.
2. COM Libraries form the Business Layer.
3. **Fidelio Database** library forms the Data Layer for Oracle DB communication.

Suite8 is a windows application, It does not require any deployment on server. The Suite8 artifacts (Windows forms and COM libraries) are copied and provided to the necessary configuration file.

Users Authentication

Overview

Authentication is the process of ensuring that people on both ends of the connection are who they say they are. Authentication is applicable not only to the entity trying to access a service but also applicable to the entity providing the service.

User Authentication

You must authenticate through the workstation by signing in to the application utilizing a unique employee Username and Password.

2

Performing a Secure Suite8 Installation

This chapter presents planning information for your Suite8 installation.

For information about installing Suite8, see the *Suite8 Installation Guide* located at http://docs.oracle.com.

Pre-Installation Configuration

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Review the Oracle Hospitality Enterprise Back Office Security Guide.
- Review the Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide.
- Create Oracle Database Tablespaces per the instructions in the *Suite8 Installation Guide* located at http://docs.oracle.com.

Post-Installation Configuration

This section explains additional security configuration steps after Suite8 is installed.

Application

Software Patches

Apply the latest Suite8 patches available on My Oracle Support.

Follow the deployment instructions included with the patch.

Database Platform

Ensure Database Access is tracked

Ensure that database login auditing is enabled regardless of the database platform that is being utilized.

Passwords Overview

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 characters long and maximum 20 characters.
2. The password must contain letters, numbers, and special characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
3. Must not choose a password equal to the last 4 passwords used.