Oracle® Hospitality Cruise Dining Management System - SilverWhere

Security Guide
Release 8.0.
E98955-02

July 2020

ORACLE

Contents

Preface

This document provides security reference and guidance for Dining Management System - SilverWhere.

Audience

This document is intended for:

- System administrators installing Dining Management System - SilverWhere.
- End users of Dining Management System - SilverWhere.

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
July 2020	• Updated the Password Overview, Password Lifetime, Configure User Accounts and Privileges, and Concurrent Sessions and Constraints.

1 Dining Management System - SilverWhere Security Overview

This chapter provides an overview of Oracle Hospitality Dining Management System - SilverWhere 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)/Secure Socket Layer (SSL), and secure passwords.
- **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 Dining Management System - SilverWhere Security

Dining Management System - SilverWhere Architecture Overview

Dining Management System - SilverWhere uses N-Tier Architecture and is a collection of applications and interfaces. They can be deployed either on shore side or ship side. It is scalable and does not have to be deployed on a single machine.

Technology

Dining Management System - SilverWhere 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 (Windows DPAPI, PBKDF2) to encrypt and store sensitive information like application user passwords, application configuration information, database user passwords.

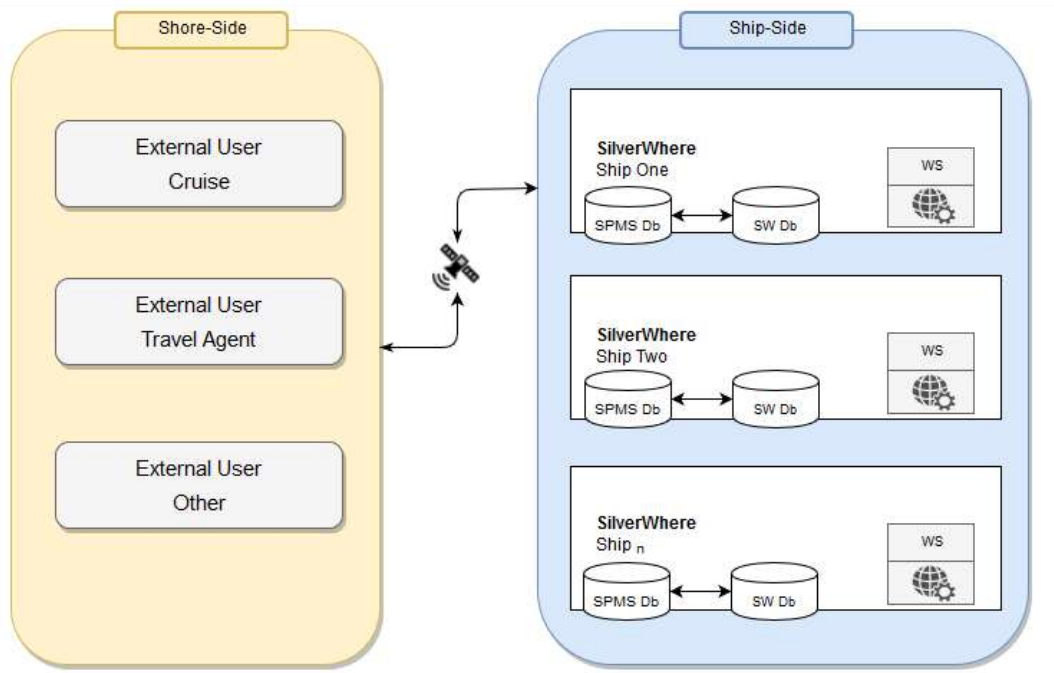

Figure 1 - SilverWhere Data flow diagram

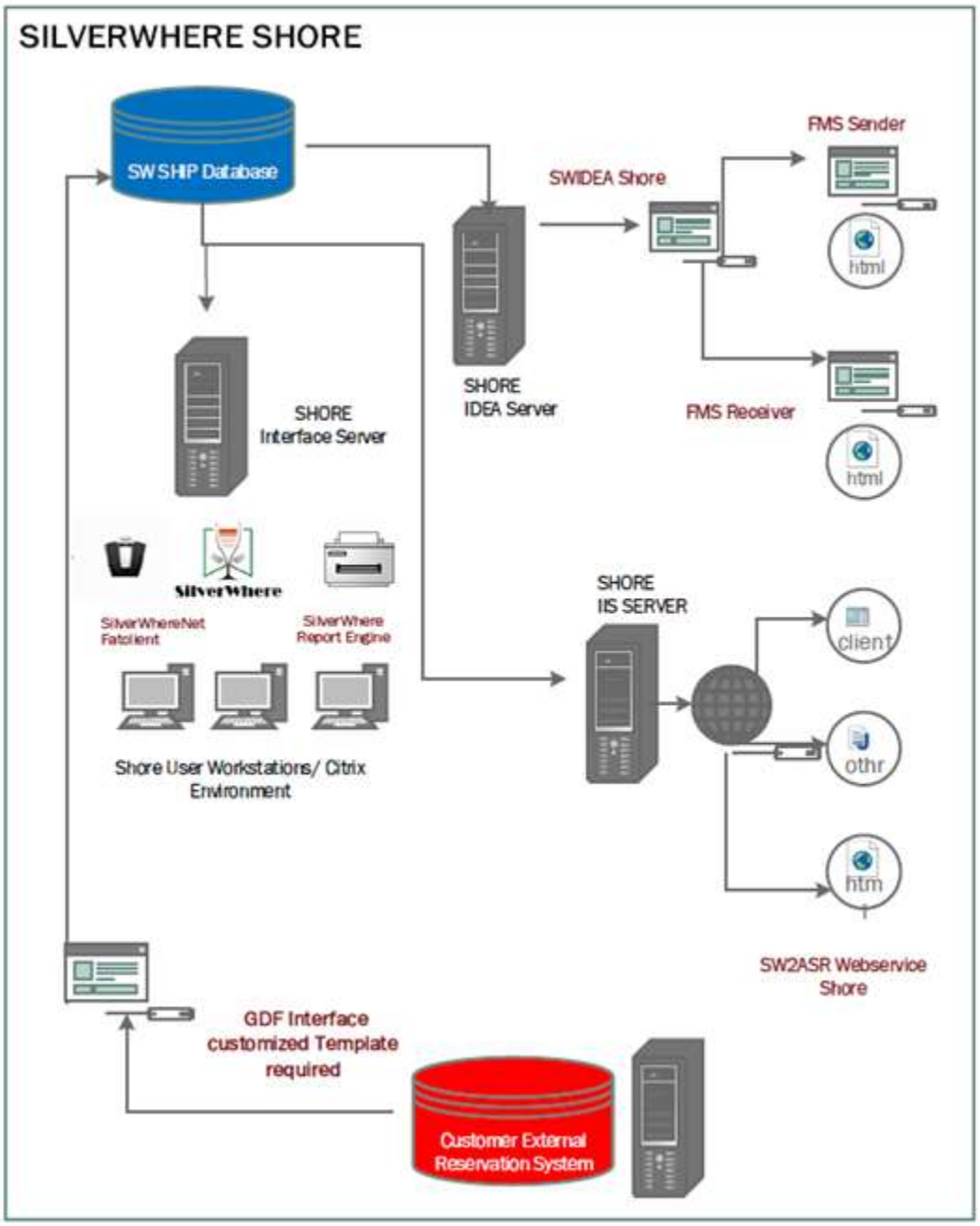

Figure 2 - SilverWhere Architecture – Shore

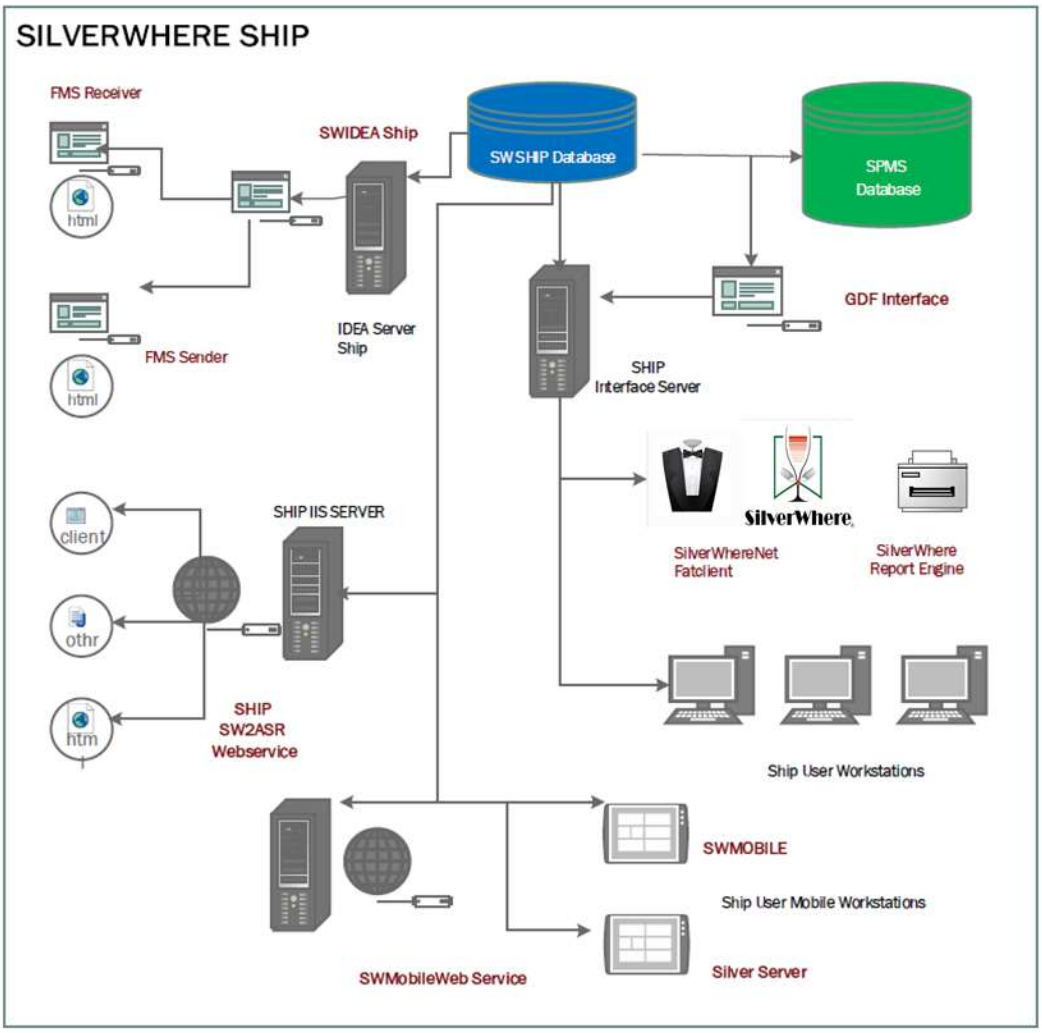

Figure 3 - SilverWhere Architecture – Ship

User Authentication

Overview

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

Client Authentication

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

Database Users

Dining Management System - SilverWhere works with both Oracle Server databases.

Understanding the Dining Management System - SilverWhere Environment

When planning your Dining Management System - SilverWhere 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 Dining Management System - SilverWhere.

The Dining Management System - SilverWhere 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.

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.

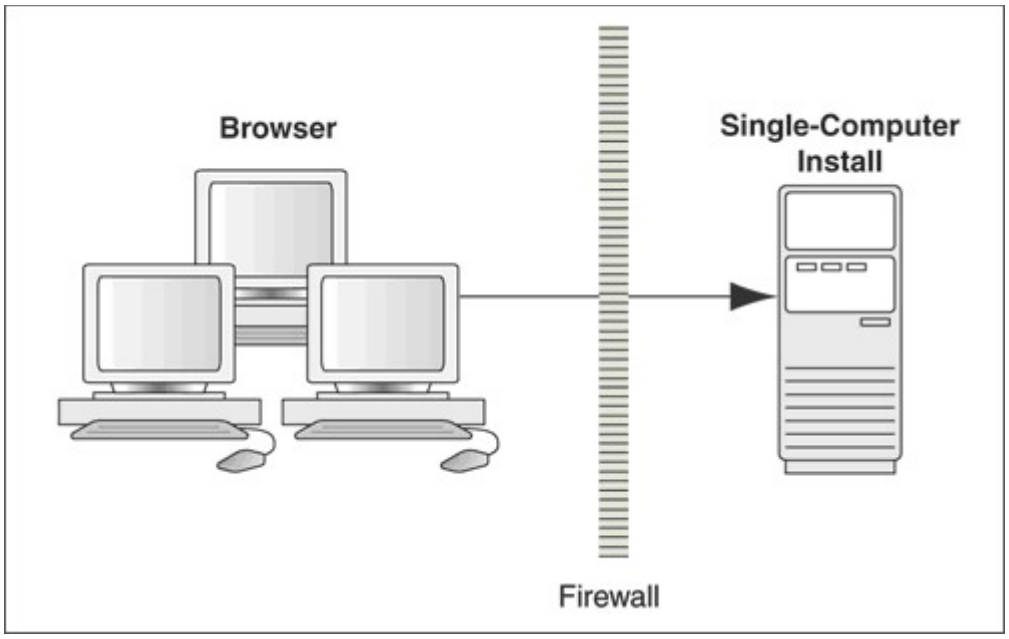

Figure 2 - Single-Computer Deployment Architecture.

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.

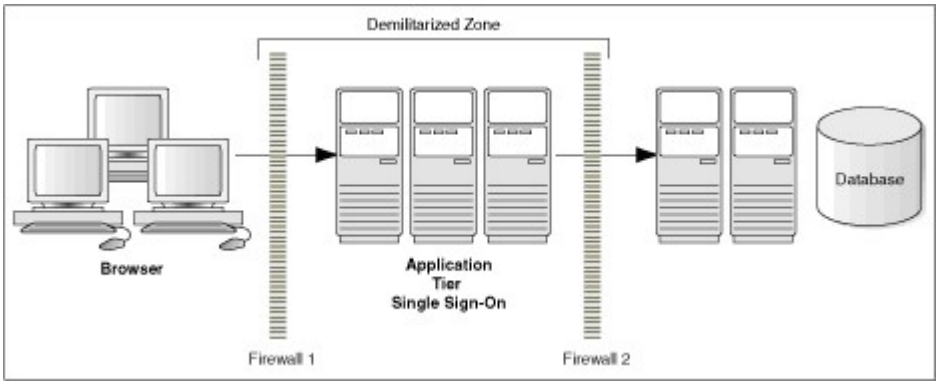

Figure 3 - Traditional DMZ View

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

Before you install the Dining Management System - SilverWhere, the operating system must be 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 Dining Management System - SilverWhere Installation

This chapter presents planning information for your Dining Management System - SilverWhere installation.

Pre-Installation Configuration

Before installation of Dining Management System - SilverWhere, perform the following tasks:

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

Dining Management System - SilverWhere 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 privilege assigned. Users without the required access might complete the installation but it may not be successful.

When creating a database, enter a complex password that adheres to the database hardening guides for all users.
The following Desktop applications are required for proper operation of the system:

- Dining Management System - SilverWhere

The following modules are required for proper operation of the system:
Basic Components for minimum functioning

Silver Server
SilverWhere
SilverWhere Report
SW Database Installer
SW Web Service

Additional Components

Silver Server Updater Service
SW Mobile Client
SW Updater
SW Updater Service

Post-Installation Configuration

This section explains the additional security configuration steps to complete after Dining Management System - SilverWhere 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 Dining Management System - SilverWhere patches available on My Oracle Support if available any. Follow the deployment instructions included with the patch.

Passwords Overview

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

Password verification functions are used to ensure that the user password meets the minimum requirements for complexity. Check and ensure the `PASSWORD_VERIFY_FUNCTION` parameter for the user profile created in the Database is not NULL.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:

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

Change Default Passwords

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

Password Lifetime

Password expiration is used to ensure that users change their passwords regularly. It also provides a mechanism to automatically disable temporary accounts. Set the PASSWORD_LIFE_TIME parameter for user profile in the Database.

Configure User Accounts and Privileges

When setting up users of the Dining Management 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.
Set INACTIVE_ACCOUNT_TIME in the profiles assigned to users to automatically lock accounts that have not logged in to the database instance in a specified number of days. It is also recommended to audit infrequently used accounts for unauthorized activities.

Concurrent Sessions and Constraints

The database user is by default have unlimited concurrent connections but may result in memory resource exhaustion or Denial-of-Service attacks. It is advised to set the `SESSIONS_PER_USER` for this. We recommend that you check for disabled constraints, and determine where applicable if they need to be disabled, deleted, or enabled as these are a potential cause for concern.