

Oracle® Hospitality Cruise Shipboard Property Management System Security Guide



Release 20.2
F44463-04
December 2023



F44463-04

Copyright © 1995, 2023, Oracle and/or its affiliates.

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 is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

1 Configure Secure Transport Layer Security for SPMS and Oracle Database Connection

Enabling TLS 1.2 for SPMS Clients and Oracle Database Connection 1-2

2 Shipboard Property Management System Security Overview

Basic Security Considerations 2-1

Overview of Shipboard Property Management Security 2-1

Understanding the SPMS Environment 2-4

Recommended Deployment Configurations 2-4

Component Security 2-6

3 Performing a Secure Shipboard Property Management System Installation

Pre-Installation Configuration 3-1

Shipboard Property Management System Installation 3-1

Web Services Installation 3-1

REST API / Web Apps Server Installation 3-2

Establishing a Connection 3-2

4 Post-Installation Configuration

Software Certificates 4-1

Password Overview 4-1

Maintaining Strong Passwords 4-1

Change Default Password 4-2

Password Lifetime 4-2

Configure User Accounts and Privileges 4-2

Concurrent Sessions and Constraints 4-2

Encryption Keys	4-2
-----------------	-----

5 Shipboard Property Management System Security

Authorization Privileges	5-1
User Security/Access Rights	5-1
Audit Trail/Application Activity Log	5-4
Change Log Trigger	5-4
Deleting a Log Trigger	5-5
Inserting a Log Trigger	5-5
Shipboard Property Management System OHC Tools	5-6
Verify Database Encrypted Data	5-7
Change Database Encryption Key	5-7
Change Password Manager	5-8
Upload Pretty Good Privacy (PGP) Key	5-9

A Appendices

Preface

This document provides security reference and guidance for the Oracle Hospitality Cruise Shipboard Property Management System (SPMS).

Audience

This document is intended for:

- Customers installing the SPMS
- Oracle Dealers
- MIS Personnel

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

<https://iccp.custhelp.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
- Screenshots 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/cruise.html>.

Revision History

Table 1 Revision History

Date	Description of Change
September 2021	Initial publication.
March 2022	Made minor grammatical changes.
October 2022	Updated the document with correct format.
December 2023	Updated new customer portal.

1

Configure Secure Transport Layer Security for SPMS and Oracle Database Connection

Reference Documents

Refer to the official published document shown below for detailed information on Oracle Advanced Security, where it describes in detail how to configure and use the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

For Oracle 12c database: <https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F>

Difference between Secure Sockets Layer and Transport Layer Security

Transport Layer Security (TLS) is an incremental version of Secure Sockets Layer (SSL) version 3.0. Although SSL was primarily developed by Netscape Communications Corporation, the Internet Engineering Task Force (IETF) took over development of it, and renamed it Transport Layer Security (TLS).

Recommended TLS Version for SPMS

TLS 1.2 and above is the recommended protocol for SPMS.

Prerequisites

1. The Oracle database server version should be **Oracle Database Enterprise Edition 12c Release**.
2. On the application machine, **Oracle Database 12c 32bit ODAC** and **12c Client** are required.
3. The Oracle public key infrastructure (PKI), which provides **Oracle Wallet** and **Oracle Wallet Manager (OWM)**, is required. The OraclePKI command is used to create keys to generate certificates. The OraclePKI command can be found in `$ORACLE_HOME/bin` folder.

Using TLS for SPMS Clients and Oracle Database Connection

Transport Layer Security (TLS) can be used in a multi tenant environment for SPMS applications. If you want to use Transport Layer Security (TLS) in a multi-tenant environment for an SPMS application, then you must ensure that the database is able to use its own wallet with its own certificates for TLS authentication.

TLS works with the core Oracle Database features such as encryption and data access controls. By using Oracle Database SSL functionality to secure communications between clients and servers, you can:

- use TLS to encrypt the connection between clients and servers.
- authenticate any client or server, to any Oracle database server that is configured to communicate over TLS.

Enabling TLS 1.2 for SPMS Clients and Oracle Database Connection

You must configure TLS 1.2 on the Oracle database server, and then the SPMS clients.

1. Configure TLS 1.2 on the Oracle Database Server.
 - Configure the Oracle wallet and use TCP/IP with SSL on the server. See [Step 1](#), [Step 3](#), and [Step 4](#)
2. Configure TLS 1.2 on the SPMS clients.
 - – When you configure SSL on the client, configure the server DNS and use TCP/IP with SSL on the client. See [Step 2](#) and [Step 5](#)
3. Log in to the Database Instance.
 - After you have completed the configuration, you are ready to log in to the database.

Step 1: Configure Oracle Wallet for Server (Database) Side

1. Open a command prompt window as a normal user.
2. Create a directory on the server machine to store the server wallet at <SERVER_WALLET>. Run the make directory command below at "C:/Oracle" folder.

```
>mkdir wallets
>cd wallets
>mkdir db
>cd db
```

Based on the sample above, the value for <SERVER_WALLET> is "C:\Oracle\wallets\db".

3. Create a wallet for the Oracle server. Create an empty wallet with auto login enabled:

```
> orapki wallet create -wallet "<SERVER_WALLET>" -pwd <password> -auto_login
```

Example: orapki wallet create -wallet "C:\Oracle\wallets\db" -pwd <password> -auto_login

4. Add a self-signed certificate in the wallet (a new pair of private/public keys is created):

```
> orapki wallet add -wallet "<SERVER_WALLET>" -pwd <password> -dn "CN=<server_machine_name>" -keysize 2048 -self_signed -validity <No. of Days>
```

Example: orapki wallet add -wallet "C:\Oracle\wallets\db" -pwd <password> -dn "CN=server1" -keysize 2048 -self_signed -validity 365

5. Check the contents of the wallet. Notice the self-signed certificate is both a user and trusted certificate.

```
> orapki wallet display -wallet "<SERVER_WALLET>" -pwd <password>
```

6. Export the certificate so it can be loaded into the client wallet later.

```
> orapki wallet export -wallet "<SERVER_WALLET>" -pwd <password> -dn
"CN=<server_machine_name>" -cert <SERVER_WALLET>\<server-certificate-
name>.crt
```

Example: orapki wallet export -wallet "C:\Oracle\Wallets\db" -pwd <password>
-dn "CN=server1" -cert C:\Oracle\wallets\db\server-cert-db.crt

7. Check whether the certificate has exported to the above directory.

Step 2: Configure Oracle Wallet for Client (Application) Side

You must create a client wallet on all SPMS client machines. Follow the steps below to create a client wallet and repeat the steps on each of the database client machines.

1. Open a command prompt window as a normal user.
2. Create a directory on the client machine to store the client wallet. Call it <CLIENT_WALLET>. Create it under the "C:\Oracle" folder.

```
>mkdir wallets
>cd wallets
>mkdir user
>cd user
```

Based on the sample above, the value for <CLIENT_WALLET> is
C:\Oracle\wallets\user

3. Create a wallet for the Oracle client. Create an empty wallet with auto login enabled:

```
> orapki wallet create -wallet "<CLIENT_WALLET>" -pwd <password> -auto_login.
```

Add a self-signed certificate in the wallet (a new pair of private/public keys is created):

```
> orapki wallet add -wallet "<CLIENT_WALLET> " -pwd <password> -dn
"CN=<client_machine_name>" -keysize 2048 -self_signed -validity <No. of
Days>
```

Note:

Ensure each client certificate has a unique name. Use the client machine name as the certificate name.

4. Check the contents of the wallet. Note that the self-signed certificate is both a user and trusted certificate.

```
> orapki wallet display -wallet "<CLIENT_WALLET>" -pwd <password>
```


5. Export the certificate, so it can be loaded into the server wallet later.

```
> orapki wallet export -wallet "<CLIENT_WALLET>" -pwd <password> -  
dn "CN=<client_machine_name>" -cert <CLIENT_WALLET>\<client-  
certificate-name>.crt
```

 **Note:**

Ensure each client certificate has a unique name, use the client machine name as the certificate name.

6. Check whether the certificate is exported to the above directory.

Step 3: Perform Clients-Server Exchange Certificate Process

These instructions are for the exchange server and client public keys. These steps must be repeated on each of the database client machines.

1. Copy <server-certificate-name>.crt from the server machine to the client machine <CLIENT_WALLET> folder.
2. Copy <client-certificate-name>.crt from the client machine to the server machine <SERVER_WALLET> folder.
3. Load the server certificate into the client wallet.

```
orapki wallet add -wallet "<CLIENT_WALLET>" -pwd <password> -  
trusted_cert -cert <CLIENT_WALLET>/<server-certificate-name>.crt
```

4. Check the contents of the client wallet. Note that the server certificate is now included in the list of trusted certificates.

```
orapki wallet display -wallet "<CLIENT_WALLET>" -pwd <password>
```

5. Load the client certificate into the server wallet.

```
orapki wallet add -wallet "<SERVER_WALLET>" -pwd <password> -  
trusted_cert -cert <SERVER_WALLET>/<client-certificate-name>.crt
```

6. Check the contents of the server wallet. Note that the client certificate is now included in the list of trusted certificates.

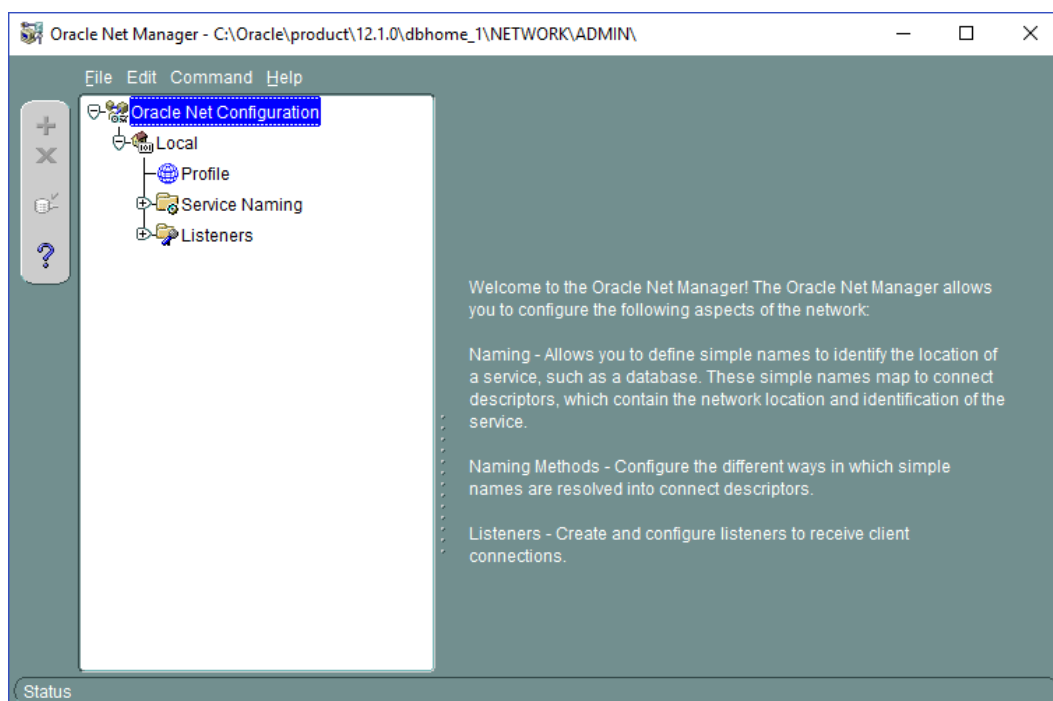
Step 4: Configure the Oracle Database to Listen For TCPS Connection

Configure the listener.ora and sqlnet.ora files on the database server using the following steps.

To configure the listener.ora file:

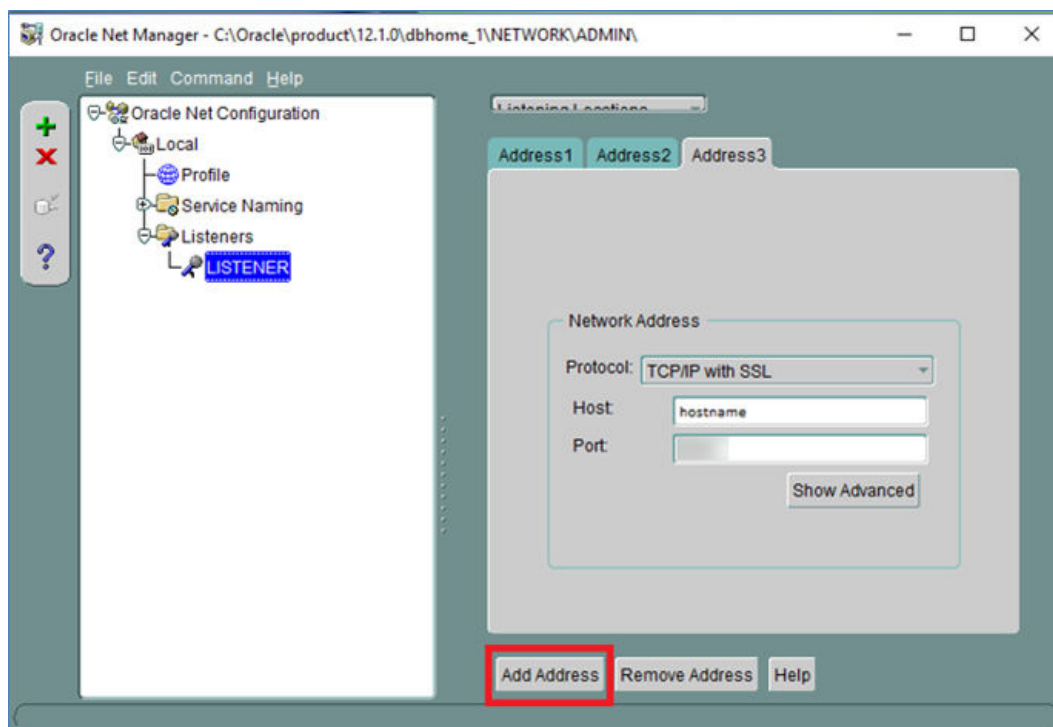
1. Launch the Net Manager Tool.

Figure 1-1 Net Manager



2. Expand the Listeners container under **Local**, and select the **Listener**.
3. Click **Add Address** and select **TCP/IP with SSL** as the protocol.
4. Enter the hostname and port as shown in the screen below.

Figure 1-2 Listener, Address Tab



5. Click **File**, and then click **Save Network Configuration** to save the setting. Below is an example of the listener.ora file

```
...
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = example.com) (PORT = <PORT
NO>))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = example.com) (PORT = <PORT
NO>))
    )
  )
...

```

To configure the sqlnet.ora file using Oracle Net Manager:

1. Click **Profile**, and then select **Network Security** from the drop-down list.
2. Select the **SSL tab**, and then select the **Server** option.
3. Enter the values as shown below:

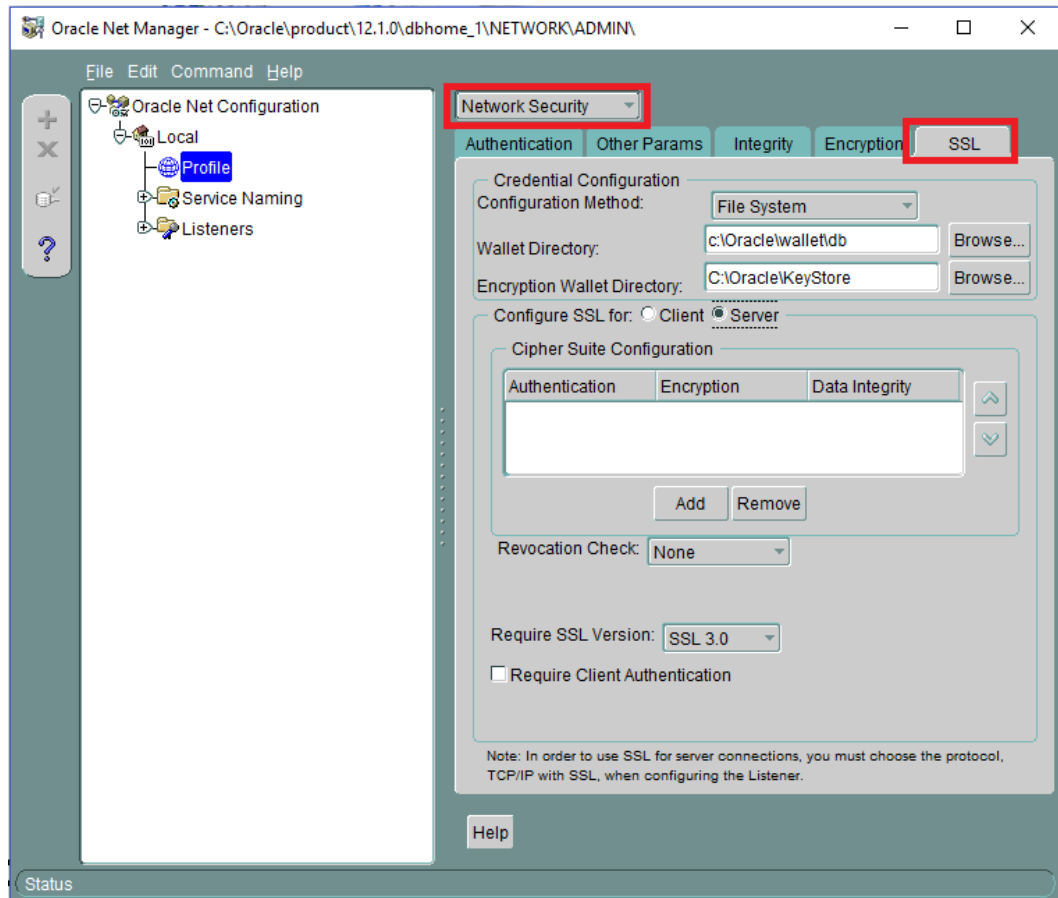
Configuration Method: File System

Wallet Directory: <SERVER_WALLET>

Configure SSL for: Server

Revocation Check: None **Require Client Authentication:** FALSE

Figure 1-3 Network Security in Net Manager



4. Click **File**, and then click **Save Network Configuration** to save. At this point, exit the Oracle Net Manager tool and ensure all changes are saved.
5. Since the Oracle Net Manager does not allow for certain values to be changed, open `<ORACLE_HOME>/network/admin/sqlnet.ora` and make sure the following properties are set to

```
SSL_VERSION = 1.2
SSL_CIPHER_SUITES= (SSL_RSA_WITH_AES_128_GCM_SHA256)
```

6. In `<ORACLE_HOME>/dbs/init.ora` make sure the following property is set to


```
_use_fips_mode=FALSE
```
7. Restart the Database Service and listener so that all the above changes takes effect. From Windows Services **Administrative Tools, Services**, restart the corresponding Database Service. The Listener can be restarted from Windows services or as shown below:

Open the command prompt and follow the below steps using **Run as Administrator**:

```
> lsnrctl stop
> lsnrctl start
```

After completing the steps, re-open the Net Manager. Below is a sample of the sqlnet.ora and listener.ora file:

```
<ORACLE_HOME>/network/admin/sqlnet.ora
...
SQLNET.AUTHENTICATION_SERVICES=(BEQ,TCPS,NTS)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 1.2
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA = (DIRECTORY = C:/Oracle/wallets/db))
  )
SSL_CIPHER_SUITES= (SSL_RSA_WITH_AES_128_GCM_SHA256)
...
<ORACLE_HOME>/network/admin/listener.ora
...
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA = (DIRECTORY = C:/Oracle/wallets/db))
  )
...
```

To configure the tnsnames.ora file:

1. Click on **Service Naming** in Net Manager.
2. Click on **Edit**, select **Create** to create a new service. Complete the **Net Service Name Wizard** as described below:

Net Service Name: <Service Name>

Select: "TCP/IP with SSL (Secure Internet Protocol)"

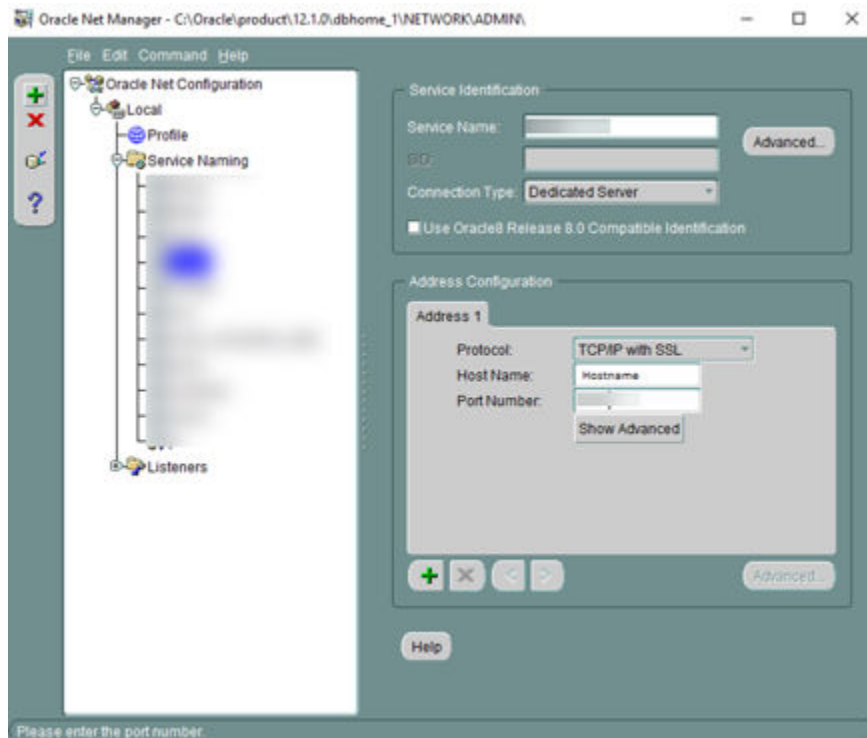
Host Name: <Host Name>

Port Number: <Port Number>

(Oracle8i or later) Service Name: <Service Name>

Connection Type: *Default database* Test the connection on page 5 of the wizard.

Figure 1-4 Net Manager Service Name



Here is the sample tnsnames.ora file:

```
...
fidelio_tcps =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = example.com) (PORT = <Port No>)))
    (CONNECT_DATA = (SERVICE_NAME = <Service_Name>))
  )
...
```

3. Click **File**, and then click **Save Network Configuration** to save.
4. Click **File**, and then click **Exit**. All server configurations have been completed.

Step 5: Configure the Oracle Client to Connect with TCPS Connection

Perform the following configuration on the machine running the SPMS application.

1. Follow the steps in [Step 4](#) for configuring the client **sqlnet.ora** file. This file is located in the <ORACLE_HOME>/network/admin folder. File contents are similar to the example below.

```
...
SQLNET.AUTHENTICATION_SERVICES=(BEQ,TCPS,NTS)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 1.2
WALLET_LOCATION =
```

```
(SOURCE =  
  (METHOD = FILE)  
  (METHOD_DATA = (DIRECTORY = C:/Oracle/wallets/user))  
)  
  
SSL_CIPHER_SUITES= (SSL_RSA_WITH_AES_128_GCM_SHA256)  
...
```

2. Follow the steps in [Step 4](#) for configuring the **tnsnames.ora** file on the client/application. This file is located in the `<ORACLE_HOME>/network/admin` folder. Below are the sample file contents:

```
FIDELIO=  
(DESCRIPTION =  
  (ADDRESS_LIST =  
    (ADDRESS = (PROTOCOL = TCPS) (HOST = example.com) (PORT = <Port  
No>))  
  )  
  (CONNECT_DATA =  
    (SERVER = DEDICATED)  
    (SERVICE_NAME = <Service Name>)  
  )  
)
```

3. Connect to the Database using SQL*Plus client with SSL.
4. Launch the SQL*Plus session from the command line, by typing the username and password as `<username>/<password>@ssl_connectstring`.

 **Note:**

To enable the IIS Server connection to the database, the wallet folder of the IIS server must give permission to IIS_IUSR to access the wallet. For further details, refer to the Oracle Database Security Guide, section “*Configuring Secure Sockets Layer Authentication*” located at: <https://docs.oracle.com/database/121/DBSEG/asossl.htm#DBSEG9665>.

2

Shipboard Property Management System Security Overview

This chapter provides an overview of the Oracle Hospitality Cruise Shipboard Property Management System security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental in order to use 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.** You 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 Sockets Layer (SSL) and secure passwords. See [Performing a Secure Shipboard Property Management 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. See Security Considerations for Developers 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>

Overview of Shipboard Property Management Security

SPMS Architecture Overview

The SPMS uses an N-Tier/3-Tier Architecture style. Most of the application components are Microsoft Windows desktop applications, interfaces, RESTful API, Progressive Web application (WPA), and a few web services used for third party integration. It is scalable since clients/interfaces, databases, and web services can be distributed onto three or more machines and does not have to be deployed on a single machine.

Technology

Shipboard Property Management System Web Services uses industry standard Simple Object Access Protocol (SOAP)/JavaScript Object Notation (JSON) to work with internal and external applications. Typically, web services are deployed and exposed on the Microsoft Internet Information Services (IIS) Webserver, and IIS provides options to secure the

communications using the Secure Sockets Layer (SSL). It also uses Transmission Control Protocol /Internet Protocol (TCP-IP) and File System for integration internally and externally. Every communication can be configured to use the Secure Sockets Layer (SSL) if required. It also uses strong encryption/hashing algorithms (Microsoft managed Rijndael, Microsoft Windows Data Protection Application Programming Interface (DPAPI), Password-Based Key Derivation Function 2 (PBKDF2)) to encrypt and store sensitive customer information, application user passwords, application configuration information, secrets, and passwords.

Figure 2-1 SPMS Network Architecture Diagram

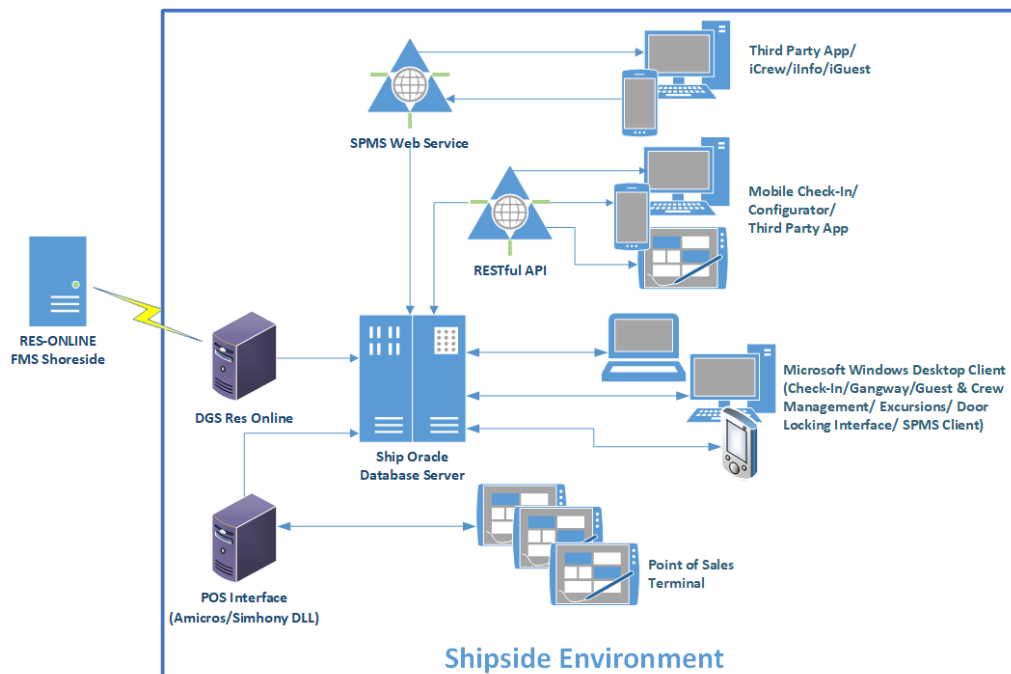
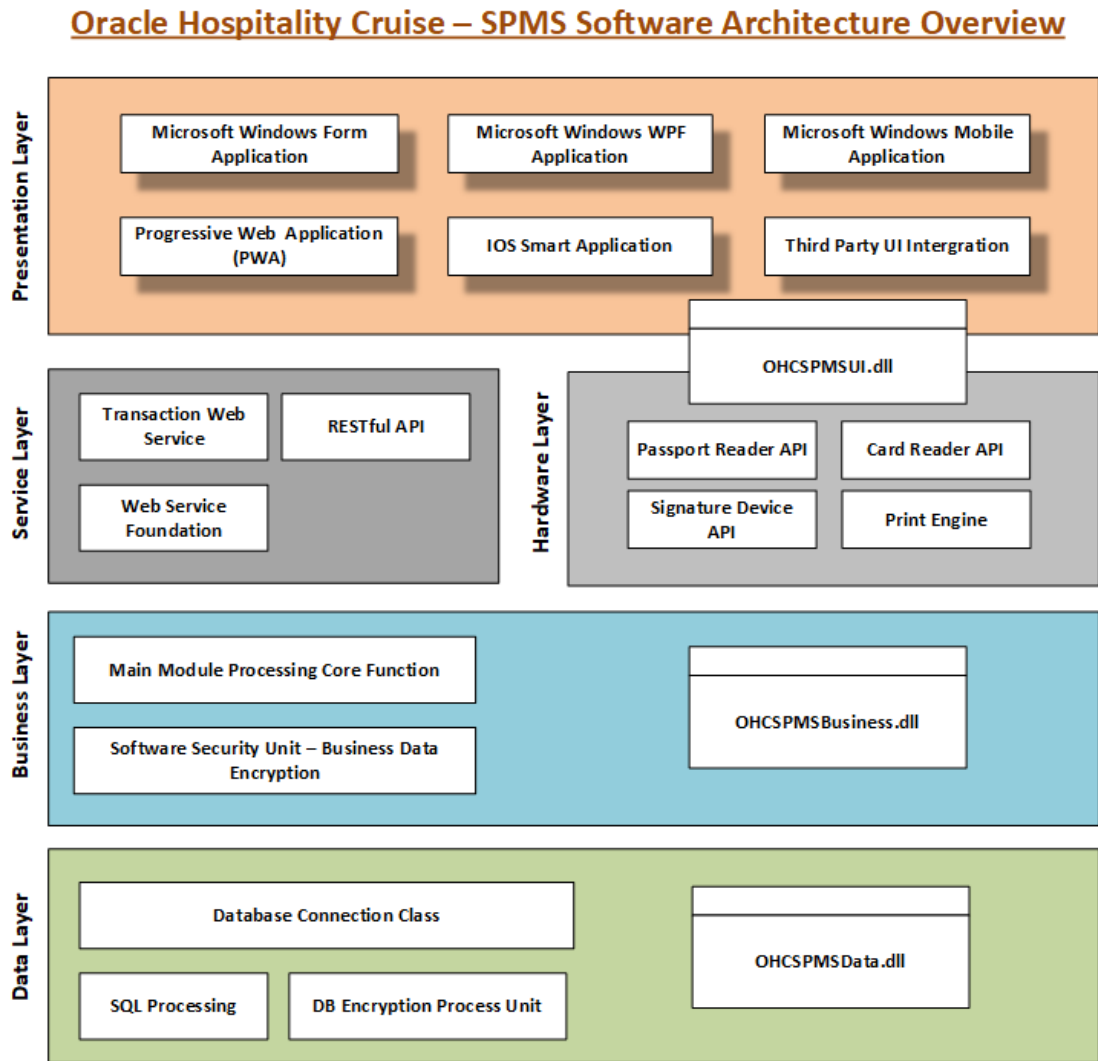


Figure 2-2 SPMS Software Architecture Diagram



User Authentication

Overview

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

Thick/Windows Desktop Client/RESTful API/PWA Authentication

All user credentials for the SPMS are stored in the database. Anyone who wishes to access the desktop client must provide a valid username and password. To ensure strict access control of Shipboard Management, always assign unique usernames and complex passwords to each user. The passwords must follow the Payment Card Industry-Data Security Standard (PCI-DSS) guidelines and must have at least 8 characters and a combination of letters and numbers.

Web Service Authentication

The Security Session ID Approach is used in the Web Services/Web Apps only. For the first request from a client, predefined credentials are passed to gain a session ID, and this session ID is used with subsequent requests throughout the session.

Database Users

The Shipboard Property Management System stores the database user password on a local machine in an encrypted format using Microsoft Windows DPAPI (Data Protection Application Programming Interface) starting from Microsoft Windows 2000 onwards.

Security Note

The Oracle database user password and Key Encryption Key (KEK) are hosted/stored on a SPMS Security Server (OHC Secure Login Web Service), deployed on the IIS web server. Clients need to connect to the Security Server once to fetch the Database user password and KEK, and store them locally in their configuration file in an encrypted form using the Microsoft Windows DPAPI method. The Client uses a password stored in the configuration file to connect to the Database. The Client will only connect to the SPMS Security Server again to fetch the password, if the Database user password is changed.

Understanding the SPMS Environment

When planning your SPMS implementation, consider the following:

- Which resources need to be protected?
 - 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?

Any of your subscriber's data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflow 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.

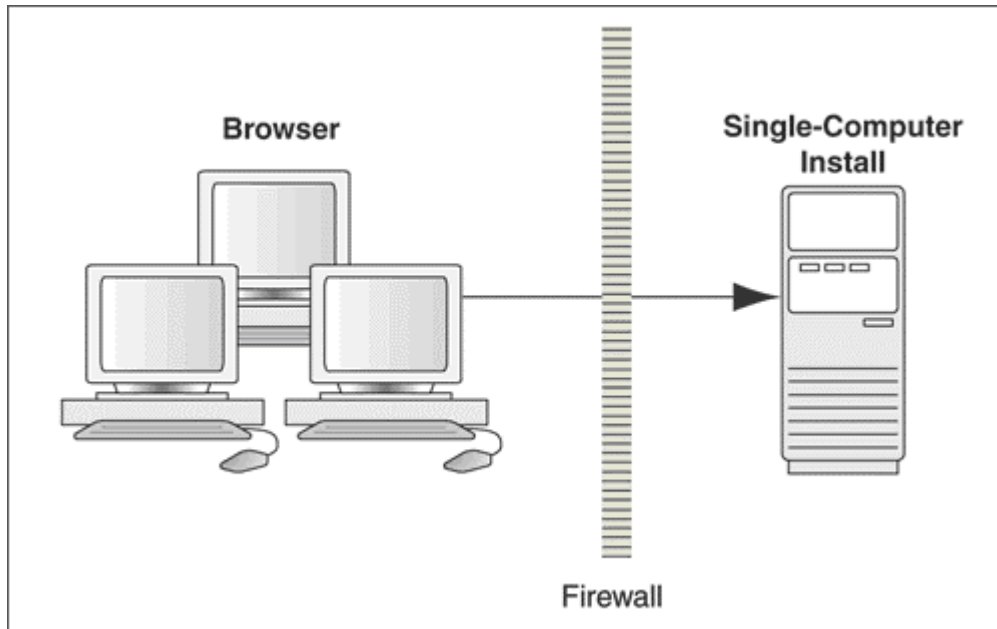
Recommended Deployment Configurations

This section describes recommended deployment configurations for the SPMS.

The SPMS can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in figure [Simple Computer Deployment Architecture](#).

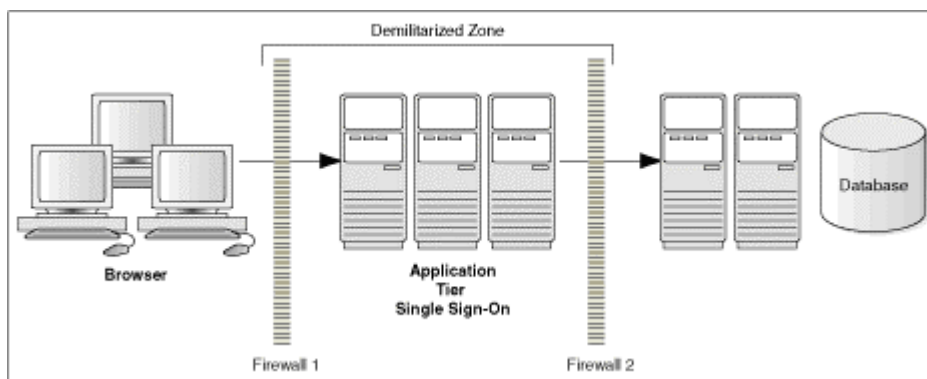
This single-computer deployment may be cost effective for small organizations; however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

Figure 2-3 Simple Computer Deployment Architecture



The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture as shown in the figure below.

Figure 2-4 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 the DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal.

- Providing intrusion containment, should successful intrusions take over processes or processors.

See [Appendix A - Shipboard Property Management System Ports Numbers](#) for more information about the SPMS network port usage.

Component Security

Operating System Security

Before installing the SPMS, 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 for:

- [Microsoft Windows Server 2012 Security](#)
- [Microsoft Windows Server 2016 Security](#)
- [Microsoft Windows Server 2019 Security](#)

Oracle Database Security

See [Oracle Database Security Guide](#) for more information about Oracle Database security.

Web Security

Use only HTTPS or Transport Layer Security (TLS) security obtained from a certification authority for the SPMS application.

3

Performing a Secure Shipboard Property Management System Installation

This chapter presents planning information for the SPMS installation.

For information about installing the SPMS, see *SPMS 20.2 Installation Guide*, available at the [Oracle Help Center](#).

Pre-Installation Configuration

Before installing the SPMS, the following tasks must be performed:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Create the required Oracle Database objects per the instructions in the *SPMS 20.2 Installation Guide* available at [Oracle Help Center](#).
- Acquire the Secure Sockets Layer (SSL) compliant security certificate from the Certification Authority.

Shipboard Property Management System Installation

You can perform a custom or a typical installation of the SPMS. Perform a custom installation to avoid installing options and products you do not need. If you choose to 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 guidelines for all users.

Before you begin, ensure these features are turned on and the required files are available.

- For a Microsoft Windows 10 user, ensure the **Microsoft .NET Framework 4.8** is turned on in Window Features before installing the Oracle Full Client and **OHC_SPMS_V20.2SETUP.exe**.
- Download the **OHC_SPMS_V20.2SETUP.exe** from the [Oracle Software Delivery Cloud](#).

Web Services Installation

This section describes the steps to install the OHC Web Services and other required Microsoft Windows components.

Installing WebServices

See section *Setting Up SPMS .Net Secure Server* and *Setting Up SPMS .Net WebServer* of *SPMS 20.2 Installation Guide* for steps to complete the installation.

REST API / Web Apps Server Installation

This section describes the steps to install the REST API/ Web Apps and other required components.

Installing REST API/ Web Apps Server

See section *Installing SPMS REST API / Web Apps Server* of *SPMS 20.2 Installation Guide* for steps to complete the installation

Cross-Origin Resource Sharing (CORS)

Put in place the Cross-Origin Resource Sharing (CORS) protocol and use the domain list to limit options for requests. Do not use an asterisk (*) as an origin value; it allows access from all hosts.

Establishing a Connection

Web Service Connection

For Symphony users:

- Ensure the Symphony Extensibility DLL version is the same as SPMS.
- Go to Symphony Properties Enterprise and select the option “*Fidelio Web Server Address*”, and then change the SPMS web service to `https://<ip address>/OHCTransactionsSevices/OHCTransactionsServices.asmx`

Web Service Database Connection

Edit the ‘**web.config**’ file in `C:\inetpub\wwwroot\OHCTransactionsService` and define the SPMS database server name under `<appSetting>`.

```
<appSettings>
  <add key="Server" value="<SERVER NAME>" />
</appSettings>
```

WebService File Path Configuration for Symphony

1. Edit the ‘**web.config**’ file in `C:\inetpub\wwwroot\OHCTransactionsService` and change the file path name where the `mi_exp.txt`, `employee.txt`, `rvc.txt`, and `AL Product Classes.txt` files will be saved.
2. Change the `--Path--` according to the path you created in the `c:\temp\folder`. The path can be the ship name or ship code and it is user-definable.

Figure 3-1 Symphony File Path


```

web.config - Notepad
File Edit Format View Help
machine.config.comments usually located in
\Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration>
  <appSettings>
    <add key="Server" value="..."/>
    <add key="DB Transaction Timeout" value="60"/>
    <add key="Debug" value="False"/>
    <add key="MenuItemFile" value="c:\temp\--Path--\mi_exp.txt"/>
    <add key="EmployeeFile" value="c:\temp\--Path--\employee.txt"/>
    <add key="RevenueCenterFile" value="c:\temp\--Path--\rvc.txt"/>
    <add key="ProductClassFile" value="c:\temp\--Path--\AL Product Classes.txt"/>
    <add key="NoneRefundableCreditMaxCount" value="5"/>
    <add key="SecureLogin" value="1..."/>
  </appSettings>

  <!--
  For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

  The following attributes can be set on the <httpRuntime> tag.
  <system.Web>
    <httpRuntime targetFramework="4.5" />
  </system.Web>

```

WebService Configuration for OPI

Edit the 'web.config' file in C:\inetpub\OHCOPIWebServices and to define the SPMS database server name (SOURCE) and password (PASSWORD) under <connectionStrings>.

```

<connectionStrings>
  <add name="OHCEntities" connectionString="metadata=<a target="_blank"
href="res://*/OHModel.csdl|res://*/OHModel.ssd|res://*/
OHModel.msl;provider=Oracle.ManagedDataAccess.Client;provider">res://*/
OHModel.csdl|res://*/OHModel.ssd|res://*/
OHModel.msl;provider=Oracle.ManagedDataAccess.Client;provider</a>
connection string=&quot;DATA SOURCE=[SOURCE];PASSWORD=[PASSWORD];PERSIST
SECURITY INFO=True;USER ID=<USER ID>&quot;;"
providerName="System.Data.EntityClient" />
</connectionStrings>

```

If Wallet is applied,

```

<connectionStrings>
  <add name="OHCEntities" connectionString="metadata=<a target="_blank"
href="res://*/OHModel.csdl|res://*/OHModel.ssd|res://*/
OHModel.msl;provider=Oracle.ManagedDataAccess.Client;provider">res://*/
OHModel.csdl|res://*/OHModel.ssd|res://*/
OHModel.msl;provider=Oracle.ManagedDataAccess.Client;provider</a>
connection string=&quot;DATA SOURCE=<IP Address>:<Port No>/<Service
Name>;PASSWORD=[PASSWORD];PERSIST SECURITY INFO=True;USER ID=<User
ID>&quot;;" providerName="System.Data.EntityClient" />
</connectionStrings>

```


4

Post-Installation Configuration

This section explains the additional security configuration steps to complete after the Shipboard Property Management System is installed.

Operating System

Turn On Data Execution Prevention (DEP)

Turn on DEP if required. Refer to the Microsoft product documentation library for instructions.

Turning off Auto Play

Turn off Autoplay 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.

Software Patches

If a patch is available, download and apply the latest SPMS patches from My Oracle Support. Follow the deployment instructions included with the patch.

Software Certificates

If a Secure Sockets Layer (SSL) certificate is required, it must be configured either on the load balancer or in the IIS web server for communication to web services. Secure Sockets Layer (SSL) usage on the SPMS Security Server is mandatory.

The Self-signed certificate should be used only if the customer fails to provide a certificate from a Certificate Authority (CA). See *SPMS Installation Guide* for information about the installation of secure certificates.

Password Overview

Configuration of the SPMS product passwords is performed at the SPMS User Security module. Administrators should adopt 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 of 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:

- The password must be at least 8 characters long.
- The password must contain letters and numbers.
- You must not select a password equal to the last three passwords used.

Change Default Password

The SPMS is installed with a default administrative user and password. You must change the default administrative user password in SPMS, following the above guidelines, after logging in for the first time.

Password Lifetime

The Shipboard Property Management System is installed with a default administrative user and password. You must change the default administrative user password in the Shipboard Property Management System, following the above guidelines, after logging in for the first time.

Configure User Accounts and Privileges

When setting up users for the SPMS application, ensure that they are assigned the minimum privilege level required to perform their job function. 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 by default has unlimited concurrent connections but this may result in memory resource exhaustion or Denial-of-Service attacks. It is advised to set the `SESSIONS_PER_USER` for this. It is recommend that you check for disabled constraints, and determine where, if applicable, they need to be disabled, deleted, or enabled as they are a potential cause for concern.

Encryption Keys

The Data Encryption Key (DEK) is used to encrypt sensitive information, and is stored securely in the database for retrieval in the encrypted form using Advanced Encryption Standard (AES) and Key Encryption Key (KEK) as Passphrases/keys.

5

Shipboard Property Management System Security

This chapter explains the Shipboard Property Management System's security features.

Authorization Privileges

Overview

Setting Authorization privileges establishes strict access control, explicitly enabling or restricting the ability to do something with a computer resource.

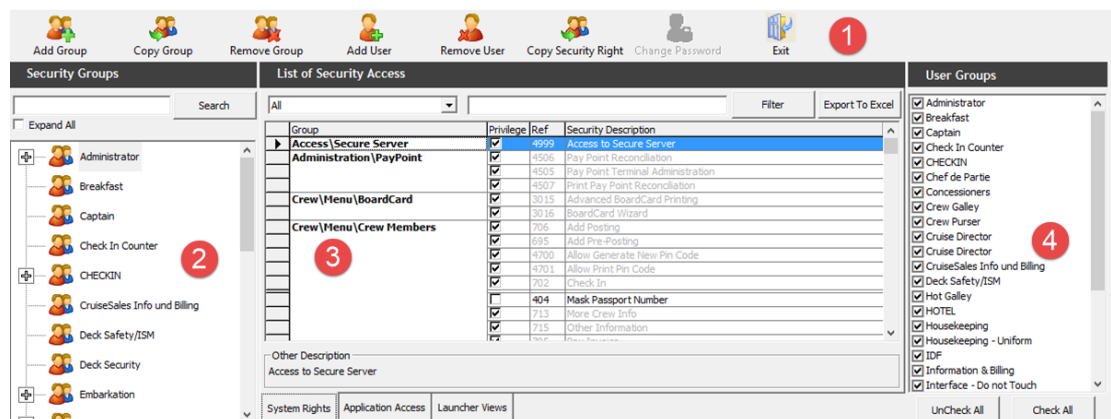
User authorization privileges are configured in the SPMS within the User Security module. The SPMS uses the simple authorization model, where each user belongs to one or more user groups, and the user has all privileges assigned to the user group(s).

The Oracle Hospitality Cruise Launch Panel is the control panel for SPMS programs and User Security Management.

User Security/Access Rights

This section describes the SPMS User Security Access by module and permission level available to users. Permission is granted at the group level instead of the individual user level.

Figure 5-1 User Security Screen



The User Security window has four sections:

1. Menu bar.
2. Security Group.

3. List of Security Access.
4. User Groups.

Accessing User Security Program

1. Launch the **OHC Launch Panel** from the C:\Program Files (x86)\Oracle Hospitality Cruise folder.
2. Navigate to the **Utilities tab** and run the **User Security** program.

Adding a User

1. Select a **Security Group** from the Security Groups list.
2. Click **Add User** from the ribbon bar.
3. In the Add User window, enter the **Login name and Description** in the User Details section and check the **User Group** associated with this user. Multiple selections of the User Group are allowed.
4. Enter the **Password** and check the password criteria in the Security section.
5. At the **Crew Name** drop-down list, select the crew profile to associate the user login and enter the information in the **various** sections, if any.
6. Click **Apply** to save the user. The newly created user is saved under the Security group container.

Figure 5-2 Add User Window

Table 5-1 Field Definition for Add User

Field	Description
Login Name	Login ID used in SPMS applications.
Login Description	User Name.
User Group	Group Access Level.
Password	User Password.
Crew Link	Link to the Crew Profile.
Buyer's Limit	Maximum spend amount allowed for goods purchases from MMS module.
Cashier Function	Enable/Disable the Cashier Function.
Cashbook Assigned	The Cashbook assigned to the user.
Operational Position	Operational Position the user is linked to.
Vendor	A user by iCrew WebServices to retrieve an excursion.

Table 5-1 (Cont.) Field Definition for Add User

Field	Description
Email Address	Email address of the user.

Changing a User Password

1. Expand the Security Group container and select the user name.
2. Click **Change Password** from the ribbon bar and enter the new password in the [User Name] field.
3. Click **Apply** to confirm the change and then click **OK** to close the dialog window.

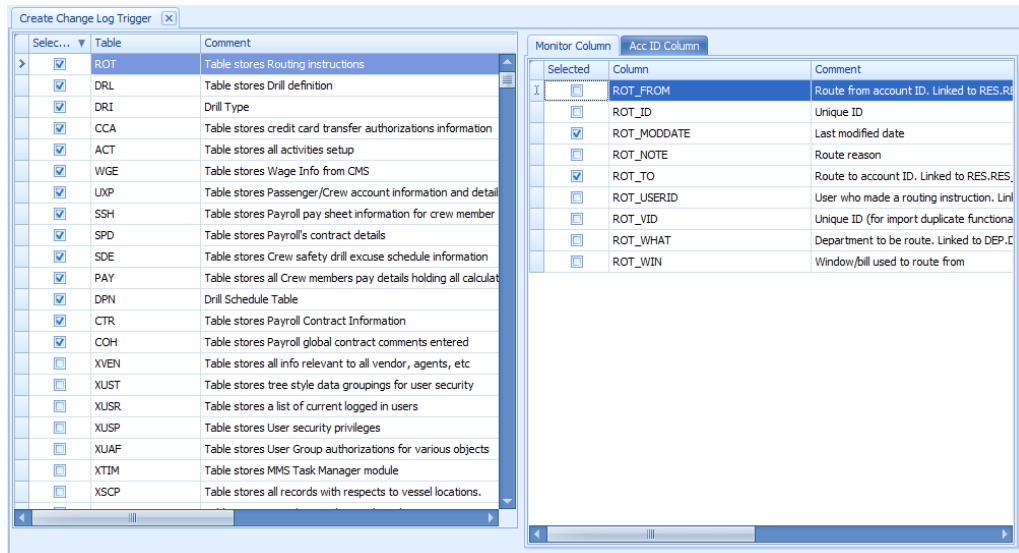
Audit Trail/Application Activity Log

This section describes the steps to create triggers to log various changes made to the database. These triggers are configured in OHC Tools.exe.

Change Log Trigger

The following function triggers a change log activity when changes are made to the selected fields and stores the log in the ADU table.

Figure 5-3 Change Log Trigger



1. In the OHC Tools window ribbon bar, select **Change Log Trigger**.
2. In the Create Change Log Trigger window, check mark the table on the left pane and then navigate to **Monitor Column** on the right pane.
3. In the **Monitor Column**, check mark the fields for changes to be logged into the ADU table and then navigate to the Acc ID Column tab.

4. In the Acc ID Column tab, check mark the field to write into the ADU_ACC_ID.
5. Click the **Create Change Log Trigger** at the ribbon bar to create the trigger. To add more table fields repeat the above steps.

Deleting a Log Trigger

This function creates a trigger to log data deletion activities of any value from the selected field into SDR table.

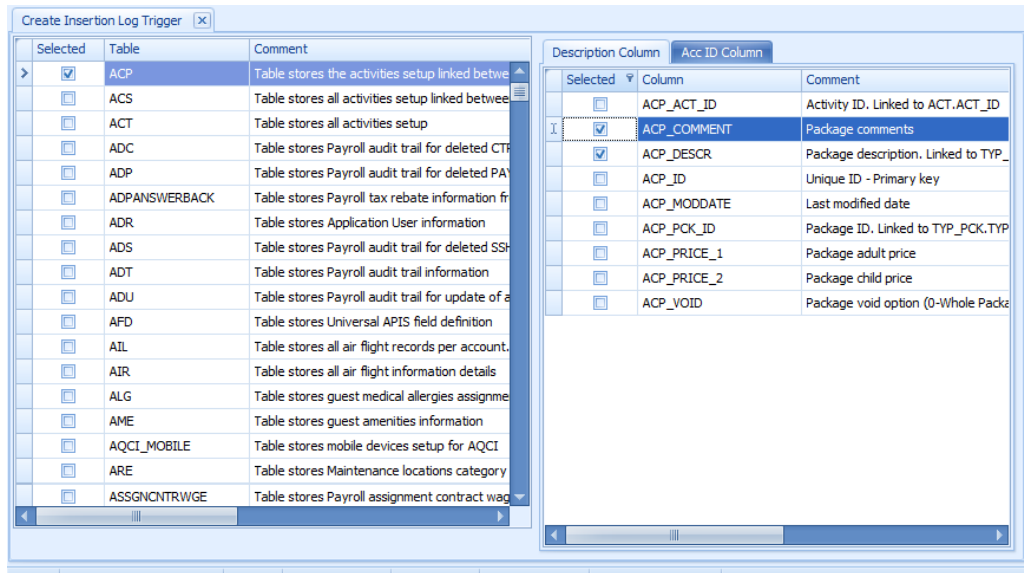
1. In the OHC Tools window ribbon bar, select the **Delete Log Trigger**.
2. In Create Deletion Log Trigger window, check mark the table on the left pane and then navigate to the **Description Column** on the right pane.
3. In the **Description Column**, check mark the field for changes to be to log into the SDR table and then navigate to the Acc ID column tab.
4. In the **Acc ID Column** tab, check mark the field to write into SDR_ACC_ID.
5. Click the **Create Deletion Log Trigger** on the ribbon bar to create the trigger.
6. The system prompts the total number of triggers deleted and created/uploaded. Click **OK** to continue. To add more table fields, repeat the above steps.

Inserting a Log Trigger

This function creates a trigger to log data insertion activities of any value for selected fields into the SIR table.

1. In the OHC Tools window ribbon bar, select the **Insertion Log Trigger**.
2. In the Create Insertion Log Trigger window, check mark the table on the left pane and then navigate to the **Description Column** on the right pane.
3. In the **Description Column**, check mark the field for changes to be logged into the SIR table and navigate to the **Acc ID Column** tab and check mark the field value to write into the SIR_ACC_ID.
4. Click the **Create Insertion Log Trigger** on the ribbon bar. The system prompts you with the total number of triggers deleted and created/uploaded.
5. Click **OK** to continue. Repeat the above steps for more table fields to be added.

Figure 5-4 Insertion of Log Trigger

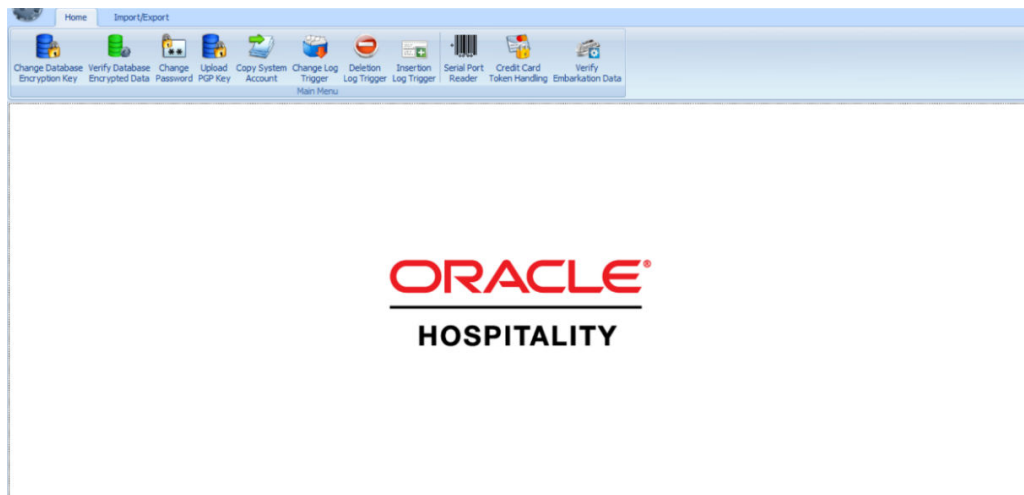


Shipboard Property Management System OHC Tools

The OHC Tools is used in the Shipboard Property Management System to encrypt and store sensitive information. The customer can select the sensitive data to encrypt and store.

1. Launch **OHC Tools.exe**.
2. At the login screen, enter your login credentials.
3. After the authentication is successful, you have access to the application and the screen shown below is visible.
4. Select the Change Database Encryption Key from the ribbon bar.

Figure 5-5 OHC Tools Main Page

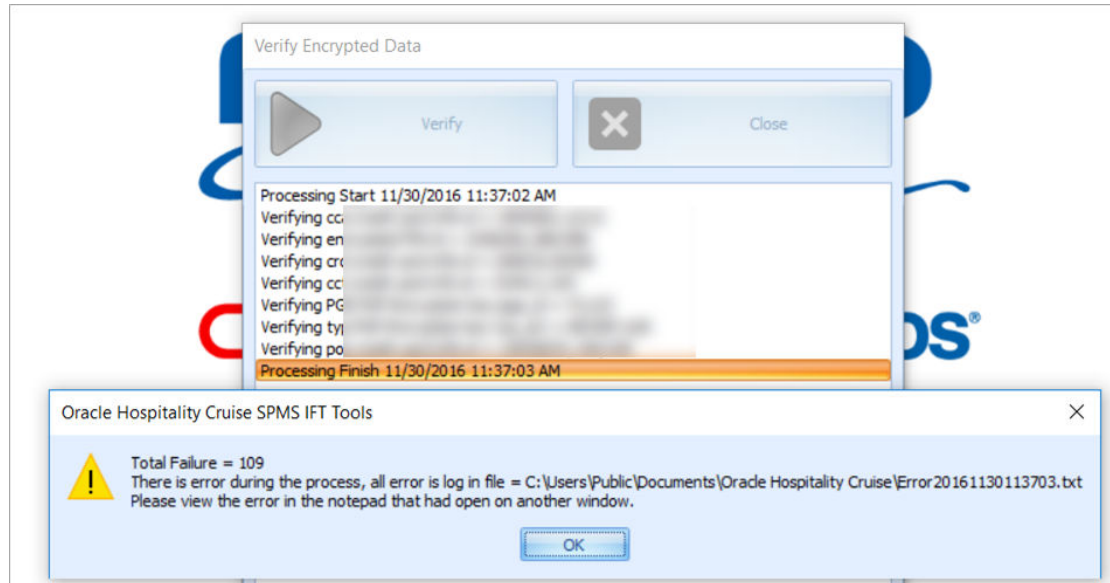


Verify Database Encrypted Data

The **Verify Database Encrypted Data** function verifies the encrypted data and confirms that the encryption can be changed before performing *Change Encryption Key*.

Verifying Encrypted Data

Figure 5-6 Verify Database Encrypted Data



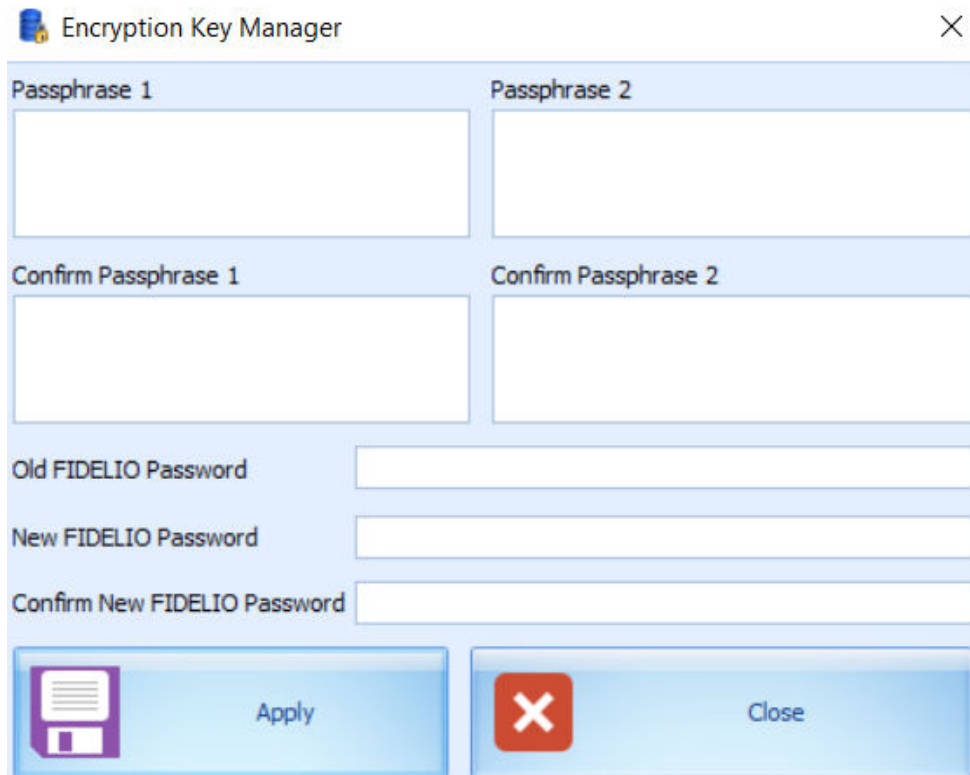
1. Log into **OHC Tools** and select **Verify Database Encrypted Data** from the ribbon bar.
2. On the Verify Encrypted Data window, click **Verify**. If the verification returns a failed message, possibly due to invalid data, correct the error and repeat the process.
3. Click **Close** when the process finishes.

Change Database Encryption Key

The Change Database Encryption Key function allows you to secure and protect important data such as credit card information and user passwords stored in the database using an encryption method compliant to the PA-DSS policy.

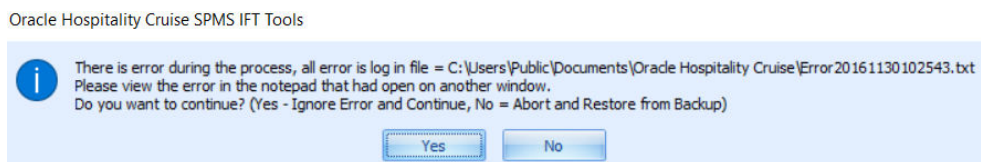
Creating an Encryption Passphrase

1. Login to **OHC Tools** and select the **Change Database Encryption Key** from the ribbon bar.
2. In the Encryption Key Manager window, enter the **Passphrase1** and **Passphrase 2, Old Fidelio password, Fidelio Password** and **Confirm** password, and then click **Apply** to proceed.

Figure 5-7 Encryption Passphrase


3. The system prompts you with the message *Please ensure there is no application currently running in order to prevent data corruption later*. Click **OK** to continue.

The program prompts you with a request to stop all running applications if any are running. A backup up process is performed on tables needing to be re-encrypted at the change encryption key. If the data is found to be corrupted during the encryption process, the system continues the process and prompts you with a warning at the end of the process and then generates an error log.

Figure 5-8 Encryption Error Confirmation


4. At the prompt, select **Yes** to continue replacing the encryption key or **No** to roll back the process by restoring the backup. The Passphrase is saved in OHCSecurity.par with a one-year validity from the date of encryption.

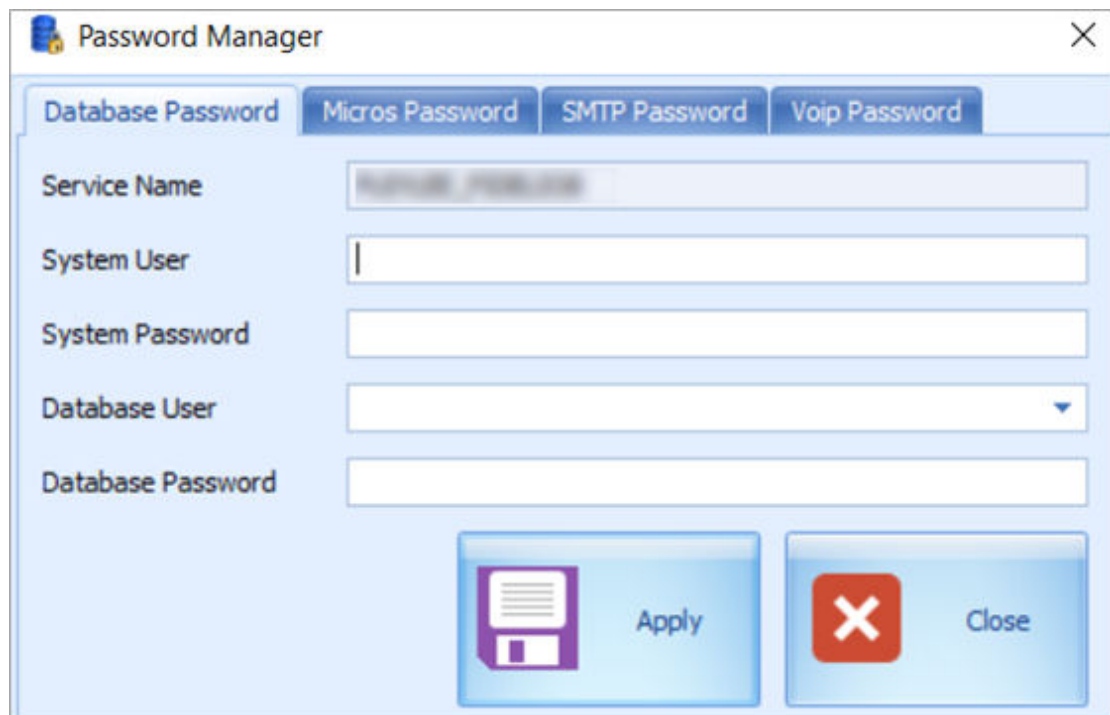
Change Password Manager

The Change Password function changes the database password, including the MICROS, SMTP, and VOIP passwords, and prevents users from changing the passwords directly from external database tools.

 **Note:**

The User is *not* allowed to change the Ship's database password when OHC QCI Sync application is running and requires a user granted with the Database privilege.

Figure 5-9 Password Manager



1. On the OHC Tools window, select **Change Password** from the ribbon bar.
2. On the Password Manager window, enter the **System User**, **System Password**, **Database User** and **Database Password**. Passwords must meet the password specification.
3. Click **Apply** to update the database password and save to *OHCSecurity.par*.
4. Repeat the above steps to change the password for MICROS, SMTP and VOIP.

Upload Pretty Good Privacy (PGP) Key

The Upload Pretty Good Privacy (PGP) Key is a function used to upload the Public Key (.pkr) and Private Key (.skr), a key pair for functionality that requires a PGP Key. For example, Payroll, Credit Card, DGS Resonline, and Data Import handling.

A key pair can only be generated using third-party tools such as PortablePGP and FileAssurity OpenPGP. Refer to the *Payment Application Data Security Standard (PA-DSS) User Guide* for more information.

For Credit Card processing, the Ship sends the public key to the credit card provider and in return, receives a public key from the provider.

1. On the OHC Tools window, select **Upload PGP Key** from the ribbon bar.
2. On the PGP Key Uploader window Credit Card tab, click **Browse** of the Public Key to select a *.pkr* file to upload. To upload a Private Key, click **Browse** of Private Key to select a *.skr* file.
3. Enter the **Key Passphrase** if the key is generated with a specific passphrase.
4. Click **Upload** to upload the keys. The system prompts *Key upload is done successfully* when the upload completes and both the keys are stored in the TYP_PGP table.
5. For DGS Credit Card handling, a key version is required.

 **Note:**

The PGP Key has an expiry date and you must generate a new PGP Key and re-upload to the database after a reminder is prompted. The program does not allow reuse of the same PGP Key.

A

Appendices

Appendix A — Shipboard Property Management System Port Numbers

Below is a list of port numbers used in the Shipboard Property Management System.

Table A-1 Supported Interface Port Numbers

Interface Type	Protocol	Port Number	Configurable
PABX	TCP	20001	No
Door Encoding	TCP	20002	No
Credit Card	TCP	20003	No
Interactive TV	TCP	20004	No
VIP/Loyalty	TCP	20005	No
Async Data Purge (ADPI)	TCP	20006	No
Paging	TCP	20007	No
Dining Interface	TCP	20008	No
Ship CC Interface	TCP	50000	Yes

Appendix B — Secure Deployment Checklist

The following security checklist is included to guide you on how to 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 workaround.
 - 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.