Oracle® Hospitality Cruise Shipboard Property Management System
Security Guide
Release 8.0
E85217-05

July 2020
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

Configure Secure Transport Layer Security for SPMS and Oracle Database Connection ......................................................... 9

Shipboard Property Management System Security Overview .......... 19

Performing a Secure Shipboard Property Management System Installation ................................................................. 25
Pre-Installation Configuration ................................................................. 25
Shipboard Property Management System Installation ............................. 25
Web Services Installation ........................................................................... 25
  Installing Automated Web Services ....................................................... 26
  Verifying an Installation Status ............................................................. 27
Establishing a connection .......................................................................... 28
  Web Service Connection ...................................................................... 28
  Web Service Database Connection ...................................................... 29
Preparing Client PC Dedicated for Database Upgrade ............................. 29
Upgrade Process ...................................................................................... 30
  Database Upgrade .............................................................................. 31
Post-Installation Configuration ................................................................. 33
  Operating System .............................................................................. 33
  Application ....................................................................................... 33
  Security Certificates .......................................................................... 34
  Passwords Overview .......................................................................... 34
  Maintaining Strong Passwords ........................................................... 34
  Change Default Passwords ................................................................. 34
  Password Lifetime ............................................................................ 34
  Configure User Accounts and Privileges .............................................. 34
  Concurrent Sessions and Constraints .................................................. 35
  Encryption Keys ................................................................................ 35
4 Shipboard Property Management System Security ............................. 36
  Authorization Privileges ...................................................................... 36
    Overview ....................................................................................... 36
  User Security/Access Rights ............................................................... 36
    Accessing User Security Program .................................................... 36
    Adding a User ................................................................................ 37
      Changing a Password ...................................................................... 38
    Audit Trail/Application Activity Log .................................................. 39
      Change Log Trigger ........................................................................ 39
      Deleting a Log Trigger ................................................................. 40
      Inserting a Log Trigger ............................................................... 40
  Shipboard Property Management System OHC Tools ......................... 41
    Change Database Encryption Key ..................................................... 42
      Creating an Encryption Passphrase ................................................ 42
    Verify Database Encrypted Data ....................................................... 43
      Verifying Encrypted Data ............................................................. 43
    Change Password .......................................................................... 44
Upload Pretty Good Privacy (PGP) Key ................................................................. 44

Appendix A - Shipboard Property Management System Ports
Numbers .............................................................................................................. 46
Figures

Figure 1-1 - Net Manager .............................................................................................................13
Figure 1-2 - Add Address .............................................................................................................13
Figure 1-3 - Network Security ....................................................................................................15
Figure 1-4 - Service Name ............................................................................................................17
Figure 2-1 - Shipboard Property Management System Network Architecture Diagram ....20
Figure 2-2 - Single Computer Deployment Architecture ...........................................................23
Figure 2-3 - Traditional DMZ View ............................................................................................23
Figure 3-1 - Webservices Files ....................................................................................................26
Figure 3-2 - Installation Failure Prompt ......................................................................................26
Figure 3-3 - Internet Connection Prompt ....................................................................................26
Figure 3-4 - Installation Selection Menu .....................................................................................27
Figure 3-5 - Successful Installation Prompt ................................................................................27
Figure 3-6 - Verification of Installation .......................................................................................28
Figure 3-7 - Upgrading WebServices .........................................................................................28
Figure 3-8 - Database Connection Setting ..................................................................................29
Figure 3-9 - Oracle Hospitality Cruise SPMS Installation ...........................................................30
Figure 3-10 - OHC Tools Main Screen .......................................................................................31
Figure 3-11 - Encryption Passphrase .........................................................................................32
Figure 4-1 - User Security Screen ...............................................................................................36
Figure 4-2 - Add User Screen ......................................................................................................37
Figure 4-3 - User Security – Add user – Security Groups .............................................................38
Figure 4-4 - User Security – Change Password ...........................................................................39
Figure 4-5 - Change Log Trigger .................................................................................................39
Figure 4-6 - Deletion Log Trigger ...............................................................................................40
Figure 4-7 - Insertion Log Trigger ...............................................................................................41
Figure 4-8 - OHC Tools Main Screen .........................................................................................42
Figure 4-9 - Encryption Passphrase ...........................................................................................42
Figure 4-10 - Error Prompt .........................................................................................................43
Figure 4-11 - Verify Database Encrypted Data .........................................................................43
Figure 4-12 - Change Password Window ...................................................................................44
Tables

Table 4-1 - Field/Description Table ................................................................. 37
Table 4-2 - Service/Protocol/Port Number Table ........................................ 46
This document provides security reference and guidance for Oracle Hospitality Cruise Shipboard Property Management System.

**Audience**

This document is intended for:
- System Administrators installing Shipboard Property Management System.
- End users of Shipboard Property Management 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 https://docs.oracle.com/en/industries/hospitality/cruise.html

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Initial publication</td>
</tr>
<tr>
<td>July 2017</td>
<td>Remove document reference link</td>
</tr>
<tr>
<td></td>
<td>Updated document format</td>
</tr>
<tr>
<td>May 2018</td>
<td>Revised Database Connection Setting screen</td>
</tr>
<tr>
<td></td>
<td>Prerequisite version changed and added OHCSpmsUtils.dll and OHCWebsockets.dll</td>
</tr>
<tr>
<td>December 2019</td>
<td>Added Configure Secure Transport Layer Security for SPMS and Oracle Database Connection.</td>
</tr>
<tr>
<td>July 2020</td>
<td>Updated the Password Overview, Password Lifetime, Configure User Accounts and Privileges, and Concurrent Sessions and Constraints.</td>
</tr>
</tbody>
</table>
1  Configure Secure Transport Layer Security for SPMS and Oracle Database Connection

Reference Documents

Please refer to the document published officially as 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:

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.

Pre-requisites

1. Oracle database server should be Oracle Database Enterprise Edition 12c Release.
2. On application machine, Oracle Database 12c 32bit ODAC and 12c Client are required.
3. Oracle public key infrastructure (PKI) which provides Oracle Wallet and Oracle Wallet Manager (OWM) is required. 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 multitenant environment for SPMS applications. If you want to use Transport Layer Security (TLS) in a multitenant environment for an SPMS application, then you must ensure that database can 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, and
- 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 Oracle Database Server
   - During installation, Oracle sets defaults on the Oracle database server and the Oracle client for SSL parameters, except the Oracle wallet location.

2. Configure TLS 1.2 on the SPMS clients
   - When you configure SSL on the client, you configure the server DNS and use TCP/IP with SSL on the client.

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 server machine to store the server wallet at `<SERVER_WALLET>`. Run 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

All SPMS client machines must create a client wallet. These steps have to be repeated for each of the database client machines. Follow the steps below to create a client wallet.

1. Open a command prompt window as a normal user.
2. Create a directory on the client machine to store the client wallet. Let’s call it <CLIENT_WALLET>. Create it under "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

4. 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: to ensure each client certificate has a unique name, use the client machine name as the certificate name

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

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

6. 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:** to ensure each client certificate has a unique name, use the client machine name as certificate name.

7. Check whether the certificate has 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 have to be repeated for each of the database client machines.

1. **Copy** `<server-certificate-name>.crt` at server machine to client machine `<CLIENT_WALLET>` folder.
2. **Copy** `<client-certificate-name>.crt` at client machine to 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. Notice 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. Notice 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 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.
2. Expand the Local, expand Listeners, and then select the Listener folder.
3. Click on Add Address and select TCP/IP with SSL as the protocol.
4. Enter the hostname and port as shown in below screen shot.
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 = 1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = example.com)(PORT = 2484))
    )
  )
...

**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 values as shown below:
   - **Configuration Method:** File System
   - **Wallet Directory:** <SERVER_WALLET>
   - **Configure SSL for:** Server
   - **Revocation Check:** None
   - **Require Client Authentication:** FALSE
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 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_256_CBC_SHA256)

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

   _use_fips_mode=FALSE

7. Restart Database Service and listener so all the above changes to take effect. From Windows Services **Administrative tools, Services**, restart the corresponding Database Service. The Listener can be restarted from either Windows services or as shown below:

   Open the command prompt and **Run as Administrator**

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

---

**Figure 1-3 - Network Security**

[Image of Oracle Net Manager with Network Security settings]
After completing the steps, reopen the Netmanager. Below is a sample of the sqlnet.ora & 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_256_CBC_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, and then 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: 2484
   (Oracle8i or later) Service Name: <Service Name>
   Connection Type: Default database
   Test the connection on page 5 of the wizard
Here is the sample tnsnames.ora file:

```ora
...  
  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 complete.

**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 at `<ORACLE_HOME>/network/admin` folder. File contents are similar as shown below:

   ```ora
   ...  
   ```
Configure Secure Transport Layer Security for SPMS and Oracle Database Connection

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_256_CBC_SHA256)
...

2. Follow the steps in Step 4 for configuring the tnsnames.ora file on client/application. This file is located at <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 a SQL*Plus session from the command line, by typing the username and password as <username>/<password>@ssl_connectstring.

**NOTE:**

To enable IIS Server connection to the database, the wallet folder of IIS server must permit IIS_IUSR to access the wallet.
2 Shipboard Property Management System Security Overview

This chapter provides an overview of Oracle Hospitality Cruise Shipboard Property Management 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), Secure Sockets Layer (SSL) and secure passwords. See Chapter 1 Configure Secure Transport Layer Security for SPMS and Oracle Database Connection for more information. See Chapter 3 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

Shipboard Property Management System Architecture Overview

Shipboard Property Management System (SPMS) uses N-Tier/3-Tier Architecture style. Most of the application pieces are Microsoft Windows desktop applications, interfaces and few web services used for third party integration. It is scalable since clients/interfaces, database and web services can be distributed onto three or more machines and do 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 Microsoft Internet Information Services (IIS) Webserver, and IIS provides options to
secure the communication using 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 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 - Shipboard Property Management System Network Architecture Diagram
User Authentication

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

Thick/Windows Desktop Client Authentication
All user credentials for Shipboard Property Management System are stored in the database. Anyone who wishes to access the desktop clients must provide a valid username and password. To ensure strict access control of the Shipboard Management, always assign unique usernames and complex passwords to each user. Password must follow Payment Card Industry-Data Security Standard (PCI-DSS) guidelines and must be at least 8 characters long and include letters and numbers.
**Web Service Authentication**

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**

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

**Security Note**

Oracle database user password and Key Encryption Key (KEK) are hosted/stored on a Shipboard Property Management System Security Server (OHC Secure Login Web Service), deployed on the IIS web server. Clients need to connect to the Security Server one time to fetch the FIDELIO DB user password and KEK and store them locally in their configuration file in the encrypted form using the Microsoft Windows DPAPI method. The Clients uses the password stored from their configuration file to connect to the FIDELIO DB user. Clients connect to the Shipboard Property Management System Security Server again only if the FIDELIO DB user password is changed to fetch the changed password.

**Understanding the Shipboard Property Management System Environment**

When planning your Shipboard Property Management System 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?**
  
  For example, you need to protect 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 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 recommended deployment configurations for Shipboard Property Management System.

Shipboard Property Management System can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown in Figure 2-2 - 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 2-2 - Single Computer Deployment Architecture](image)

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture as shown in Figure 2-3 - Traditional DMZ View.

![Figure 2-3 - Traditional DMZ View](image)

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 Shipboard Property Management System network port usage.

Component Security

Operating System Security
Before installing the Shipboard Property Management System, 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:

• Microsoft Windows Server 2012 Security
• Microsoft Windows Server 2008 R2 Security

Oracle Database Security

Oracle Database
Refer to the Oracle Database Security Guide for more information about Oracle Database security.
3 Performing a Secure Shipboard Property Management System Installation

This chapter presents planning information for your Shipboard Property Management System installation.

For information about installing Shipboard Property Management System, see the Oracle Hospitality Cruise Shipboard Property Management System Release 8.0 Installation Guide.

Pre-Installation Configuration

Before installing the Shipboard Property Management System, perform the following tasks:

- 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 Oracle Hospitality Cruise Shipboard Property Management System Release 8.0 Installation Guide located at the Oracle Help Center (http://docs.oracle.com/en/industries/hospitality/).
- Acquire Secure Sockets Layer (SSL) compliant security certificate from Certification Authority.

Shipboard Property Management 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 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 the users.

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

- For Microsoft Windows 10 user, ensure the Microsoft .NET Framework 2 and 3.5 is turned on in Window Features before installing Oracle Full Client and OHC_SPMS_V8SETUP.exe
- For Microsoft Windows 7 user, ensure the Microsoft .NET Framework 4.5 is installed, or download a copy of the installation file from https://www.microsoft.com/en-au/download/ and manually run the offline Microsoft .NET Framework 4.5 Installer.
- Download the OHC_SPMS_V8SETUP.exe and ISSetupPrerequisites folder from https://mosemp.us.oracle.com

Web Services Installation

This section describes the steps to install the OHCWebServices and other required Microsoft Windows components.
Installing Automated WebServices

1. Download the latest WebServer.zip from the Oracle Cruise release folder.

2. Unzip the file folders into c:\Temp, and navigate to c:\temp\Net Setup\Chips\WebServer folder.

![Image of Webservices Files]

3. Right-click the **Install.bat** and select **Run as Administrator** to launch the Microsoft Windows command screen.

   If the user tries to run the batch file without an Administrator login, the system prompts a failure as shown below.

![Figure 3-2 – Installation Failure Prompt]

The System then scans for an Internet connection and proceeds with the installation when the Internet connection is established. Otherwise, the installation will abort.

![Figure 3-3 - Internet Connection Prompt]

When an Internet connection is detected, the system will prompt a selection menu.
Performing a Secure Shipboard Property Management System Installation

Figure 3-4 - Installation Selection Menu

Select one of the options and press ENTER to begin the installation.

- 1 - To install OHCTransactionsService only (This includes PDAService for OHCChips user).
- 2 - To install OHCWebServices only.
- 3 - To install both OHCTransactionsService and OHCWebServices.

4. When the system prompts ‘Completed’, press any key to close the command window.

Figure 3-5 - Successful Installation Prompt

Verifying an Installation Status

1. Launch the Internet Explorer and enter below link.
   a. For OHCTransactionsService installation: https://localhost/OHCTransactionsService/OHCTransactionsService.asmx
   b. For OHCWebServices installation: https://localhost/OHCWebServices/OHCWebServices.asmx

2. If the installation is successful, you see the same browser message similar to below screen.
Performing a Secure Shipboard Property Management System Installation

3. Run the latest Web service installer. If you have installed Webservices previously, de-installation is not required.

4. Select Yes when prompt by the system override the existing file.

Establishing a connection

Web Service Connection

For Simphony users:

- Ensure the Simphony system is upgraded to version 1.07j onwards.
- Go to Simphony Properties Enterprise and choose the option “Fidelio Web Server Address”, and then change the SPMS web service to http://1xx.xx.xx.xx/OHCTransactionsSevices/OHCTransactionsServices.asmx
Web Service Database Connection

If the database server name is not defaulted to “Fidelio”, edit the ‘web.config’ file in C:\inetpub\wwwroot\OHCTransactionsService and to define the SPMS database server name under <appSetting>.

```xml
<appSettings>
  <add key="Server" value="fidelio" />
</appSettings>
```

Figure 3-8 - Database Connection Setting

Preparing Client PC Dedicated for Database Upgrade.

1. Login to PC using an Administrator login.
2. Install Oracle Full Client on the machine dedicated to performing the database upgrade, otherwise install Oracle Data Access Components (ODAC). Contact Oracle Hospitality Cruise Customer Support for installation steps if you are unsure.
3. Ensure the Database System ID (DB SID) is the same as the DB SID in IIS Server.
4. Copy the OHC_SPMS_V8SETUP.exe into c:\temp
5. At the OHC_SPMS_V8SETUP.exe, right click and select Run as Administrator.
6. The user must run the setup file using ‘Run as Administrator’.
7. If the below component(s) is not present, the system prompts to install the missing components.
Click **Install** and follow the installation wizard to complete the setup.

After the installation completes, ensure the database connection is established by using NetManager.exe to check the connection.

Navigate to Windows Control Panel, Programs and Feature and uninstall FCruiseSetup730 from the system.

Launch Notepad.exe and create a *new* text file with one of this content:
- IP Address of IIS Server
- IIS Server Name

Save the file as securelogin.txt to the Program Files, Oracle Hospitality Cruise folder.

**Note:** The UAC setting defaults to the user setting.

## Upgrade Process

This section describes the steps to upgrade the Oracle Hospitality Shipboard Property Management System Application to Version 8.0x. See Installation Guide for detailed installation and upgrade steps.

If you are upgrading from SPMS version 7.30.87x or R7.0.0.xx,
- An SPMS Database Installer version 7.30.871 if upgrading from R7.00.0xx on Oracle 11g or 7.30.872 if you are on Oracle 12c.
- An SPMS Database Installer version 7.30.872 if upgrading from 7.30.871 and below on Oracle 11g.
Before you begin,

- Login to the dedicated Client PC for Upgrade Process using a Standard User account.
- Ensure the [#Fidelio Cruise.SPMS.Last Server=Fidelio#] is in OHCSettings.par file.

**NOTE:**

If there is more than one database to upgrade, manually copy the ohcsettings.par into Public Document, Oracle Hospitality Cruise folder, and change the SID to the database you wish to upgrade.

- The DB SID on Client PC must be the same as DB SID in IIS Server.
- Copy the following files to the C:\Program Files (x86)\Oracle Hospitality Cruise folder of the dedicated Client PC for an upgrade,
  - OHC Tools.exe
  - OHCBusiness.dll
  - OHCSPMSData.dll
  - OHCSPSMSMobile.dll
  - OHCSPMSUI.dll
  - OHCSPMSUtils.dll
  - OHCWebSockets.dll

**Database Upgrade**

1. Login to the client PC as a standard user.
2. Run OHC Tools.exe version 8.0.x and click Upgrade DB to 8.0 at the ribbon bar.

![Figure 3-10 - OHC Tools Main Screen.](image)

3. In the Encryption Key Manager window, enter the Passphrase1 and Passphrase 2, Old Fidelio password, Fidelio Password and Confirm password.
4. Click **Apply** to proceed. The system will prompt *'The new passphrase has been changed…'* when the encryption completes.

After the program is upgraded to 8.0, all programs other than OHC Launch Panel and OHC Updater will be removed from **XAPP** table.

5. Double-click the **OHC Database Installer.exe** to execute the upgrade and follow the instructions of the upgrade wizard.

6. When the application upgrade completes, navigate to C:\Program Files (x86)\Oracle Hospitality Cruise folder and launch the **OHC Launch Panel** and login using a *'Bypass Updater'*.  

7. In the Launch Panel program, manually add these SPMS applications and DLLs to the respective group by pressing **F12** and select the group from the drop-down list.
   - **Utilities group**
     - Updater Watchdog.exe
   - **System Files**
     - OHCPMSUI.dll
     - OHCWebSockets.dll
   - **REGASM Files**
     - CRUFLFC.dll
     - OHCPMSData.dll
     - OHCPMSBusiness.dll
     - OHCPMSMobile.dll
     - OHCPMSUtils.dll

8. At the Launch Panel, Utilities tab, update the Launch Panel, Updater, and UpdateAgent program to the last executable by right-clicking the program and select Properties, then click **Update file** and **OK** to save.

9. Manually add the programs to the Property Management tab.

10. Exit the OHC Launch Panel program.
11. Re-login to OHC Launch Panel without Bypass Updater to update all the programs.

**NOTE:**

A program **OHC UpdaterWatchdog** is added to monitor and ensure the **OHC Updater** remains active in the Task Manager, enabling the latest program to be downloaded from XAPP. If the Standard User is not able to connect to the OHC Updater, restart the PC or switch user to Administrator, and manually restart **OHC Updater** in Task Scheduler.

12. Re-enter all previously saved special passwords in SPMS Parameter. For example: Cabin Change Password, Overwrite Limit Password, Cabin Status Change Password, and Credit Card merchant password in Credit Card Merchant Setup.

13. Verify the following passwords are saved in **OHCSecurity.par**. Otherwise, manually update the password using **OHC Tools, Change Password** function.

- VOIP Password
- SMTP Password
- MICROS Password
- Credit Card merchant password

After the program is upgraded to 8.0, all programs other than OHC Launch Panel and OHC Updater will be removed from **XAPP** table.

**Post-Installation Configuration**

This section explains the additional security configuration steps to be completed after the Shipboard Property Management System has been installed.

**Operating System**

**Turn On Data Execution Prevention (DEP)**


**Turning off Auto Play**


**Turning Off Remote Assistance**


**Application**

**Software Patches**

If available, apply the latest Shipboard Property Management System patches available on My Oracle Support. Follow the deployment instructions included with the patch.
Security Certificates

Secure Sockets Layer (SSL) certificate must be configured if required either on the load balancer or in the IIS web server for communication to web services.

Secure Sockets Layer (SSL) usage on Shipboard Property Management System Security Server is mandatory. A self-signed certificate should be used only if the customer fails to provide a certificate from a Certificate Authority (CA). Refer to the Oracle Hospitality Cruise Shipboard Property Management System Installation Guide for information about the installation of secure certificates.

Passwords Overview

The configuration of the Shipboard Property Management System product passwords is performed in the Shipboard Property Management System 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 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:

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

Change Default Passwords

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.

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 the user profile in the Database.

Configure User Accounts and Privileges

When setting up users of the Shipboard Property Management System 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 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.

**Encryption Keys**

Data Encryption Key (DEK) is used to encrypt the sensitive information, and it is stored securely in the database for retrieval in the encrypted form using Advanced Encryption Standard (AES) and Key Encryption Key (KEK) as Passphrase/key.
This chapter reviews the Shipboard Property Management System 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 Shipboard Property Management System within the User Security module. Shipboard Property Management System uses simple authorization model, where each user belongs to one more user groups, and the user gets all the privileges assigned to the user group(s).

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

User Security/Access Rights
This section describes the Shipboard Property Management System User Security Access by module and permission level available to users. Permission is granted at the group level instead of the individual user level.

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

Figure 4-1 – User Security Screen
3. The User Security window has four sections,
   a. Menu bar
   b. Security Group
   c. List of Security Access
   d. User Groups

**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, Description** in the User Details section and check the **User Group** associated with this user. Multiple selections of User Group is allowed.
4. Enter the **Password** and check the password criteria in the Security section.
5. Select the **Crew Name** from the drop-down list to associate this user login to the crew profile and enter the information in the **Various** section, if any.
6. Click **Apply** to save the user.

![Add User Screen](image)

**Figure 4-2 - Add User Screen**

**Table 4-1- Field/Description Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td>Login ID used in SPMS applications.</td>
</tr>
<tr>
<td>Login Description</td>
<td>User Name</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Group</td>
<td>Group Access Level</td>
</tr>
<tr>
<td>Password</td>
<td>User Password</td>
</tr>
<tr>
<td>Crew Link</td>
<td>Link to Crew Profile</td>
</tr>
<tr>
<td>Buyer’s Limit</td>
<td>Maximum spend amount allowed for goods purchases from MMS module.</td>
</tr>
<tr>
<td>Cashier Function</td>
<td>Enable/Disable Cashier Function.</td>
</tr>
<tr>
<td>Cashbook Assigned</td>
<td>Cashbook assignment</td>
</tr>
<tr>
<td>Operational Position</td>
<td>Operational Position user is link to.</td>
</tr>
<tr>
<td>Vendor</td>
<td>A user by iCrew WebServices to retrieve an excursion.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Email address of the user.</td>
</tr>
</tbody>
</table>

To view the newly created user, expand the Security group container.

![Security Groups](Image)

**Figure 4-3 – User Security – Add user – Security Groups**

**Changing a Password**

1. Expand the Security Group container and select the user name.
2. Click **Change Password** from the ribbon bar. In the Change Password for the [User Name] window, enter the new password.
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 and these triggers are configured in OHC Tools.exe

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

1. In OHC Tools window, select **Change Log Trigger** from the ribbon bar.
2. In Create Change Log Trigger window, select the table on the left pane and then navigate to **Monitor Column** on the right pane.
3. In the **Monitor Column**, select the fields for changes to be log into ADU table and then navigate to **Acc ID Column** tab.
4. In **Acc ID Column** tab, check the field to write into **ADU_ACC_ID**.
5. Click **Create Change Log Trigger** at the ribbon bar to create the trigger. Repeat the above steps for more table field to be added.

**Deleting a Log Trigger**

This function creates a trigger to log data deletion activities of the selected field. Any value deleted from these fields will log into SDR table.

![Figure 4-6 - Deletion Log Trigger](image)

1. At the Oracle Hospitality Cruise Tools window, select **Delete Log Trigger** from the ribbon bar.
2. At the Create Deletion Log Trigger window, check the table on the left pane and then navigate to **Description Column** on the right pane. In the **Description Column**, check the field for changes to be to log into the SDR table and then navigate to **Acc ID** column tab.
3. At the **Acc ID Column** tab, check the field to write into **SDR_ACC_ID**.
4. Click **Create Deletion Log Trigger** at the ribbon bar to create the trigger.
5. The system prompts the total number of triggers deleted and created/upload. Click **OK** to continue. Repeat the steps for more table fields to be added.

**Inserting a Log Trigger**

This function creates a trigger to log data insertion activities of the selected field. Any value deleted from these fields will log into SIR table.
At the OHC Tools window, select **Insertion Log Trigger** from the ribbon bar.

At the Create Insertion Log Trigger window, check the table on the left pane and then navigate to **Description Column** on the right pane. In the **Description Column**, check the field for changes to be log into **SIR** table and navigate to **Acc ID Column** tab and check the field value to write into **SIR_ACC_ID**.

Click **Create Insertion Log Trigger** at the ribbon bar. The system prompts the total number of triggers deleted and created/upload.

Click **OK** to continue. Repeat the above steps for more table fields to be added.

**Shipboard Property Management System OHC Tools**

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

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

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

Creating an Encryption Passphrase

1. Login to OHC Tools and select 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, then click Apply to proceed.

3. The system will prompt ‘Please ensure there is no application is currently running in order to prevent data corruption later’. Click OK to continue. The program will prompt a request to stop all running applications if any. When the change encryption
key begins, the program performs a backup process on tables needed to be re-encrypt. If data found to be corrupted during the encryption process, the system will continue the process and prompts a warning at the end of the process and generate an error log.

Figure 4-10 - Error Prompt

4. At the prompt, choose to 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 one-year validity from the date of encryption.

Verify Database Encrypted Data

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

Verifying Encrypted Data

1. Login to OHC Tools and select Verify Database Encrypted Data from the ribbon bar.
2. At the Verify Encrypted Data window, click Verify. The Verify Database Encryption Data will verify the data in table USR, PAR, RES, POS, TYP (PGP Key), CRD, CCT, CCA, and USP.
3. If the verification returns a failed message, possibly due to invalid data, correct the error and repeat the process.
4. Click Close when the process finishes.

Figure 4-11 - Verify Database Encrypted Data
Change Password
The Change Password function changes the database password, including the MICROS, SMTP and VOIP password 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.

![Password Manager Window](image)

**Figure 4-12 - Change Password Window**

1. At OHC Tools window, select **Change Password** from the ribbon bar.
2. At the Password Manager window, enter the **System User**, **System Password**, **Database User** and **Database Password**, and the password must meet the password specification.
3. Click **Apply** to update the database password and save it 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 *Payment Application Data Security Standard (PA-DSS) User Guide* for more information.

For the Credit Card process, the Ship will send the public key to the credit card provider and in return, receives a public key from the provider.

1. At the OHC Tools window, select **Upload PGP Key** from the ribbon bar.
2. At the PGP Key Uploader window Credit Card tab, click **Browse** next to Public Key to select a .pkr file to upload. To upload a Private Key, click **Browse** next to 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.

   For DGS Credit Card handling, a key version is required.

---

**NOTE:**

The PGP Key has an expiry date and the user must generate a new PGP Key and re-upload to the database after a reminder is prompt. The program does not allow reuse of the same PGP Key.
Appendix A - Shipboard Property Management System Ports Numbers

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

**Table 4-2 - Service/Protocol/Port Number Table**

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