Oracle® Hospitality Cruise Shipboard Property Management System
Security Guide
Release 8.0
E85217-02

July 2017
# Contents

**Figures** ......................................................................................................................... 5  
**Tables** .......................................................................................................................... 6  
**Preface** ........................................................................................................................... 7  
  - Audience .................................................................................................................. 7  
  - Customer Support ................................................................................................. 7  
  - Documentation ....................................................................................................... 7  
  - Revision History .................................................................................................... 7  

1 **Shipboard Property Management System Security Overview** ............ 8  
  - Basic Security Considerations ........................................................................ 8  
  - Overview of Shipboard Property Management Security ............................... 8  
    - Shipboard Property Management System Architecture Overview .......... 8  
    - Technology ........................................................................................................... 8  
    - User Authentication ........................................................................................... 10  
  - Understanding the Shipboard Property Management System Environment ... 11  
  - Recommended Deployment Configurations ................................................ 12  
  - Component Security ............................................................................................ 13  
    - Operating System Security ............................................................................. 13  
    - Oracle Database Security ................................................................................ 13  

2 **Performing a Secure Shipboard Property Management System Installation** .............................................................. 14  
  - Pre-Installation Configuration .......................................................................... 14  
  - Shipboard Property Management System Installation .................................... 14  
  - Web Services Installation ................................................................................... 15  
    - Installing Automated WebServices ................................................................. 15  
    - Verifying an Installation Status ...................................................................... 16  
  - Establishing a connection .................................................................................. 17  
    - Web Service Connection ................................................................................ 17  
    - Web Service Database Connection .............................................................. 18  
  - Preparing Client PC Dedicated for Database Upgrade ................................. 19  
  - Upgrade Process .................................................................................................. 20  
    - Database Upgrade ............................................................................................ 21  
  - Post-Installation Configuration .......................................................................... 23  
    - Operating System ............................................................................................. 23  
    - Application ....................................................................................................... 24  
    - Security Certificates .......................................................................................... 24
### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Shipboard Property Management System Network Architecture Diagram</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Single Computer Deployment Architecture</td>
<td>12</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Traditional DMZ View</td>
<td>12</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>Webservices Files</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2-2</td>
<td>Installation Failure Prompt</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2-3</td>
<td>Internet Connection Prompt</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2-4</td>
<td>Installation Selection Menu</td>
<td>16</td>
</tr>
<tr>
<td>Figure 2-5</td>
<td>Successful Installation Prompt</td>
<td>16</td>
</tr>
<tr>
<td>Figure 2-6</td>
<td>Verification of Installation</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2-7</td>
<td>Upgrading WebServices</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2-8</td>
<td>End Point address</td>
<td>18</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Database Connection Setting</td>
<td>19</td>
</tr>
<tr>
<td>Figure 10</td>
<td>– Oracle Hospitality Cruise SPMS Installation</td>
<td>20</td>
</tr>
<tr>
<td>Figure 11</td>
<td>OHC Tools Main screen</td>
<td>21</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Encryption Passphrase</td>
<td>22</td>
</tr>
<tr>
<td>Figure 13</td>
<td>– User Security screen</td>
<td>26</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Add User Screen</td>
<td>27</td>
</tr>
<tr>
<td>Figure 15</td>
<td>– User Security – Add user – Security Groups</td>
<td>28</td>
</tr>
<tr>
<td>Figure 16</td>
<td>– User Security – Change Password</td>
<td>28</td>
</tr>
<tr>
<td>Figure 17</td>
<td>– Change Log Trigger</td>
<td>29</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Deletion Log Trigger</td>
<td>30</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Insertion Log Trigger</td>
<td>31</td>
</tr>
<tr>
<td>Figure 20</td>
<td>– OHC Tools Main screen</td>
<td>32</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Encryption Passphrase</td>
<td>32</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Verify Database Encrypted Data</td>
<td>34</td>
</tr>
<tr>
<td>Figure 23</td>
<td>– Change Password window</td>
<td>34</td>
</tr>
<tr>
<td>Figure 24</td>
<td>– PGP Key Uploader</td>
<td>35</td>
</tr>
</tbody>
</table>
Tables

Table 1 - Field/Description Table ........................................................................................................27
Table 2 - Service/Protocol/Port Number Table ................................................................................36
Preface

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 http://docs.oracle.com/en/industries/hospitality/

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>
</tbody>
</table>
1 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 2 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](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 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 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?
  o You need to protect customer data, such as credit-card numbers.
  o You need to protect internal data, such as proprietary source code.
  o 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 - Single Computer Deployment Architecture*.

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

*Figure 2 - Single Computer Deployment Architecture*

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

*Figure 3 - Traditional DMZ View*
The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the Intranet, thus forming a buffer between the two. Firewalls separating DMZ zones 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

Prior to installing Shipboard Property Management System, it is essential that the operating system is 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.
2 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

Prior to 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 privileges assigned. No other users have the required access to successfully complete the installation.

When creating a database, enter a complex password that adheres to the database hardening 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 ISSetupPrerequites 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.

   ![Webservices Files](image)

   **Figure 2-1 - Webservices Files**

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

   ![Installation Failure Prompt](image)

   **Figure 2-2 – Installation Failure Prompt**

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

   ![Internet Connection Prompt](image)

   **Figure 2-3 - Internet Connection 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.

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

Select one of the option 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.

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

If the installation is successful, you see the same browser message similar to below screen.
2. Run the latest Web service installer. If you have installed Webservices previously, de-installation is not required.
3. Select Yes when prompt by the system override the existing file.

**Establishing a connection**

**Web Service Connection**

For internal users who wish to run the Demo Application,

1. Copy the configuration file \OHCDemoApp.exe.config and executable file \OHCDemoApp.exe into the C:\Program Files (x86)\Oracle Hospitality Cruise folder.
2. Open the configuration file and edit the EndPoint Address to point to the web server address.

```xml
<client>
  <endpoint
    address="http://192.168.30.52/OHCTransactionsService/OHCTransactionsService.asmx"
    binding="basicHttpBinding"
    bindingConfiguration="FidelioSPMSWS.FidelioSPMSWSSoap"
    contract="FidelioSPMSWS.FidelioSPMSWSSoap"
    name="FidelioSPMSWSSoap" />
</client>
```

![Figure 2-8 - End Point address](image)

3. For Simphony users:
   - Ensure the Simphony system is upgraded to version 1.07j onwards.
   - Go to Simphony Properties Enterprise and choose option “Fidelio Web Server Address”, and then change the SPMS web service to `http://1xx.xx.xx.xx/OHCTransactionsServices/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 define the SPMS database server name under `<appSettings>`.

```xml
<appSettings>
  <add key="Server" value="fidelio" />
</appSettings>
```
Preparing Client PC Dedicated for Database Upgrade.

1. Login to PC using an Administrator login.
2. Install Oracle Full Client on the machine if the machine is dedicated to perform 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 \temp
5. At the OHC_SPMS_V8SETUP.exe, right click and select Run as Administrator. The user must run the setup file using ‘Run as Administrator’.
6. If below component(s) is not present, the system prompts to install the missing components.
7. Click **Install** and follow the installation wizard to complete the setup.

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

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

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

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

**Note:** The UAC setting is default to user setting.

**Upgrade Process**

This section describes the steps to upgrade the Oracle Hospitality Shipboard Property Management System Application to Version 8.0x.

**Note:** For users operating on **R7.00.00xx** version, you must run OHC Database Installer version **7.30.871** before continuing.

For users operating on version below **7.30.871**, you must upgrade your database to version **7.30.871** before continuing.
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 upgrade,
  - OHC Tools.exe
  - OHCBusiness.dll
  - OHCSPMSData.dll
  - OHCSPMSMobile.dll
  - OHCSPMSUI.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 11 - 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.

Once 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 respective group by pressing **F12** and select the group from the drop-down list.
   - **Utilities group**
     - OHC Updater Watchdog.exe
   - **System Files**
     - OHCSPMSData.dll
     - OHCSPMSBusiness.dll
     - OHCSPMSUI.dll
     - OHCSPMSMobile.dll
   - **REGASM file**
     - CRUFLFC.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

Once 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 load balancer or in IIS web server for communication to web services.

Secure Sockets Layer (SSL) usage on Shipboard Property Management System Security Server is mandatory. 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 Shipboard Property Management System product passwords is performed in Shipboard Property Management System User Security module. Administrators should adopt a strong password policy after initial installation of the application and review the policy periodically.

Maintaining Strong Passwords
Ensure that passwords adhere to the following strength requirements:

- 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. 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 of the Shipboard Property Management System application, ensure that they are assigned the minimum privilege level required to perform their job function.

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 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.
The User Security window has four sections,
   a. Menu bar
   b. Security Group
   c. List of Security Access
   d. User Groups

Adding a User
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.
Table 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>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.
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 [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.
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.
1. In Oracle Hospitality Cruise Tools window, select **Delete Log Trigger** from the ribbon bar.

2. In 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. In **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 field 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.
1. In OHC Tools window, select Insertion Log Trigger from the ribbon bar.
2. In 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.
3. Click Create Insertion Log Trigger at the ribbon bar. The system prompts the total number of triggers deleted and created/upload.
4. Click OK to continue. Repeat the above steps for more table field 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 a 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 application, 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.

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.

   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 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:** User is *not* allowed to change the Ship’s database password when OHC QCI Sync application is running.

1. In OHC Tools window, select **Change Password** from the ribbon bar.
2. In Password Manager window, enter the **System User**, **System Password**, **Database User** and **Database Password** and password *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.

---

**Note:** Function requires a User granted with Database privilege.

---

**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 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. In OHC Tools window, select **Upload PGP Key** from the ribbon bar.
2. In 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.

---

**Figure 24 - PGP Key Uploader**

---

**Note:** The PGP Key has an expiry date and the user must generate a new PGP Key and re-upload to the database once a reminder is prompt. The program does not allow reuse of 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 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>