Oracle® Hospitality Cruise Shipboard Property Management System

Security Guide

Release 8.0

E85217-05

July 2020

Contents

Figures

Tables

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 https://docs.oracle.com/en/industries/hospitality/cruise.html

Revision History

Date	**Description of Change**
March 2017	• Initial publication
July 2017	• Remove document reference link • Updated document format
May 2018	• Revised Database Connection Setting screen • Prerequisite version changed and added OHCSPMSUtls.dll and OHCWebsockets.dll
December 2019	• Added Configure Secure Transport Layer Security for SPMS and Oracle Database Connection.
July 2020	• Updated the Password Overview, Password Lifetime, Configure User Accounts and Privileges, and Concurrent Sessions and Constraints.

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:

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

Difference between Secure Sockets Layer and Transport Layer Security

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

Recommended TLS Version for SPMS

TLS 1.2 and above is the recommended protocol for SPMS.

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.

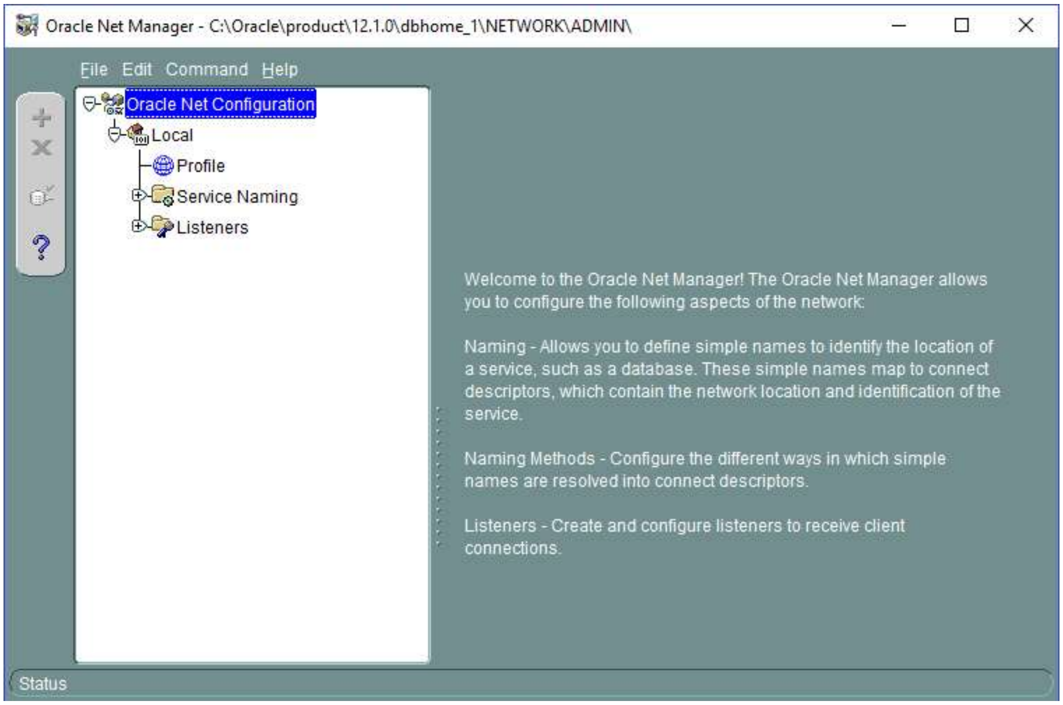
   ```
   orapki wallet add -wallet "<SERVER_WALLET>" -pwd <password>
   -trusted_cert -cert <SERVER_WALLET>/<client-certificate-
   name>.crt
   ```
6. Check the contents of the server wallet. Notice that the client certificate is now included in the list of trusted certificates.

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**.



Oracle Net Manager - C:\Oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN\

Welcome to the Oracle Net Manager! The Oracle Net Manager allows you to configure the following aspects of the network:

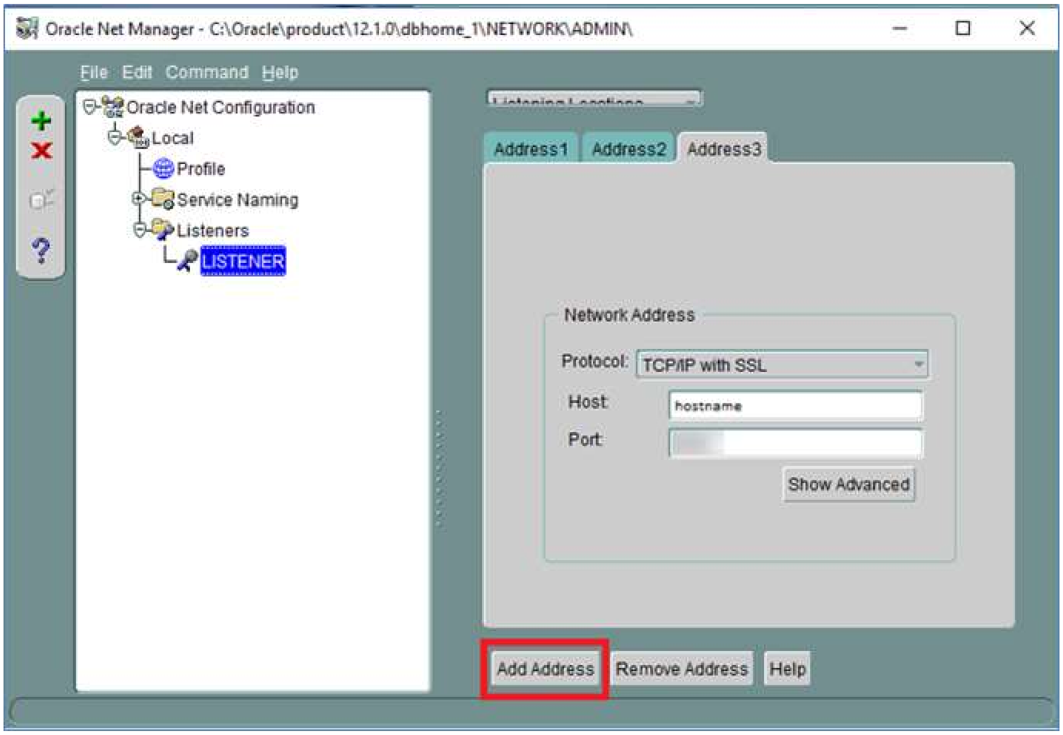
Naming - Allows you to define simple names to identify the location of a service, such as a database. These simple names map to connect descriptors, which contain the network location and identification of the service.

Naming Methods - Configure the different ways in which simple names are resolved into connect descriptors.

Listeners - Create and configure listeners to receive client connections.

Figure 1-1- Net Manager

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.



Oracle Net Manager - C:\Oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN\

Protocol: TCP/IP with SSL

Host: hostname

Port:

Figure 1-2 - Add Address

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:

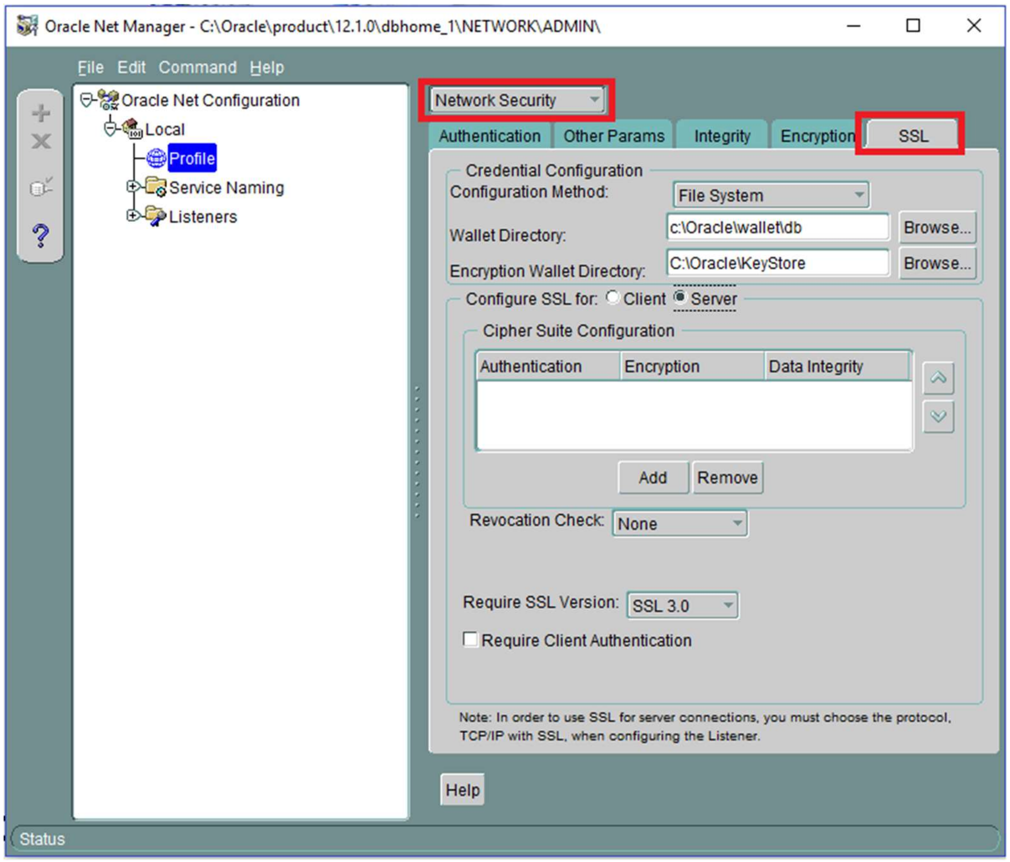
   Configuration Method: *File System*

   Wallet Directory: *<SERVER_WALLET>*

   Configure SSL for: *Server*

   Revocation Check: *None*

   Require Client Authentication: *FALSE*



Oracle Net Manager - C:\Oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN\

Network Security

Credential Configuration

Configuration Method: File System

Wallet Directory: c:\Oracle\wallet\db

Encryption Wallet Directory: C:\Oracle\KeyStore

Configure SSL for: ○ Client ● Server

Cipher Suite Configuration

Authentication	Encryption	Data Integrity

Revocation Check: None

Require SSL Version: SSL 3.0

□ Require Client Authentication

Note: In order to use SSL for server connections, you must choose the protocol, TCP/IP with SSL, when configuring the Listener.

Figure 1-3 - Network Security

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
   ```

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*

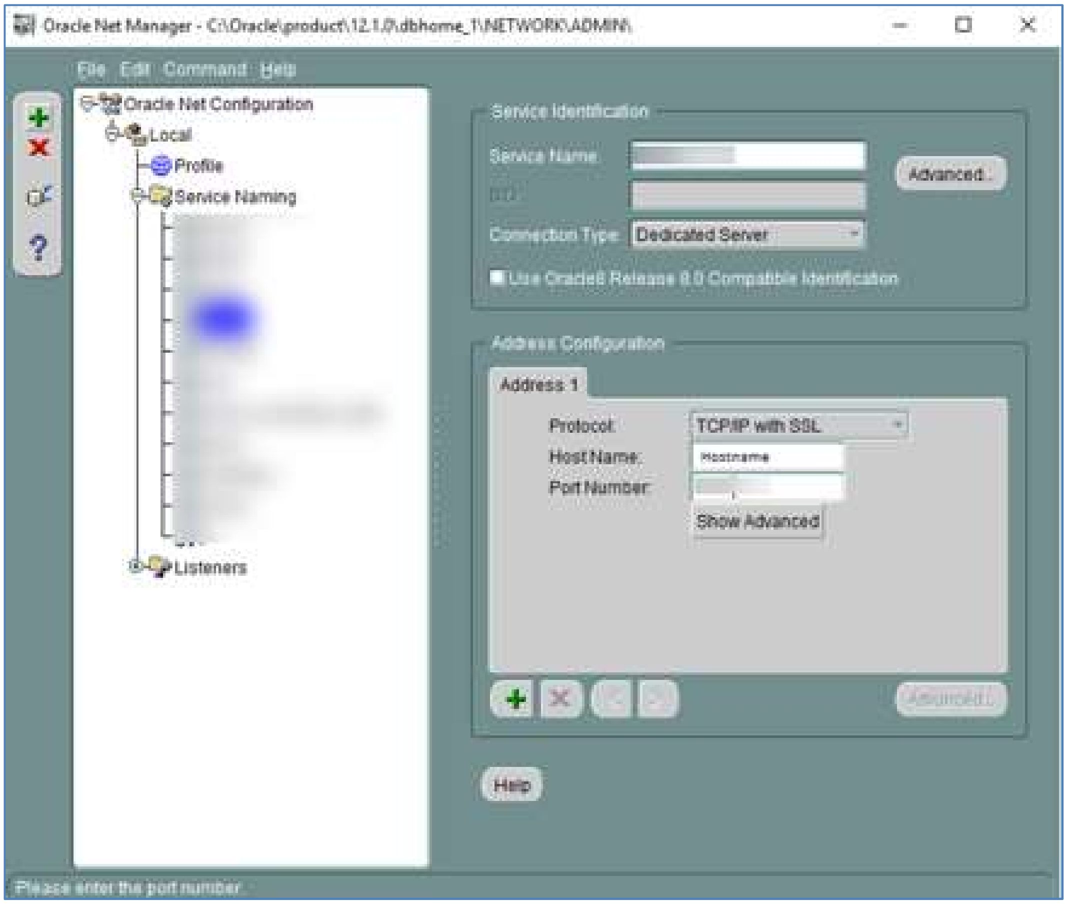
   (Oracle8i or later) Service Name: *<Service Name>*

   Connection Type: *Default database*

   Test the connection on page 5 of the wizard

Here is the sample tnsnames.ora file:

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



Oracle Net Manager - C:\Oracle\product\12.1.0\dbhome_1\NETWORK\ADMIN\

Service Name:

SID:

Connection Type: Dedicated Server

□ Use Oracle8 Release 8.0 Compatible Identification

Address 1

Protocol: TCP/IP with SSL

Host Name: Hostname

Port Number:

Show Advanced

Please enter the port number.

Figure 1-4 -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:

```
...
```

```
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.
>
> For further details, refer to Oracle Database Security Guide, section “Configuring Secure Sockets Layer Authentication” located at https://docs.oracle.com/database/121/DBSEG/asossl.htm#DBSEG9665.

2 Shipboard Property Management System Security Overview

This chapter provides an overview of 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.

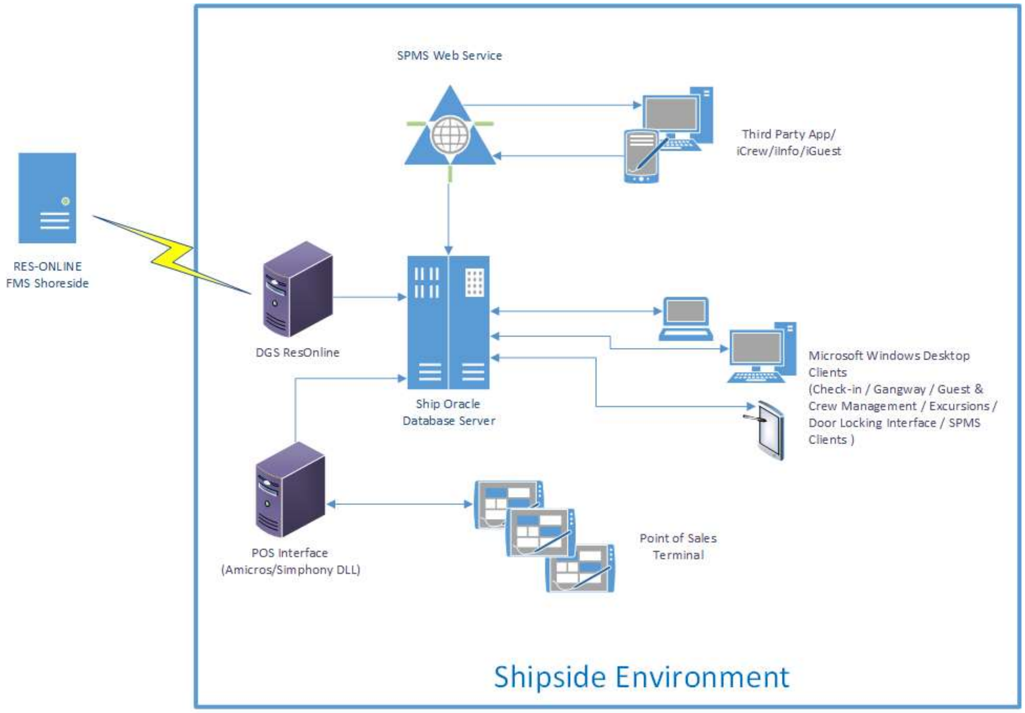


Figure 2-1 - Shipboard Property Management System Network Architecture Diagram

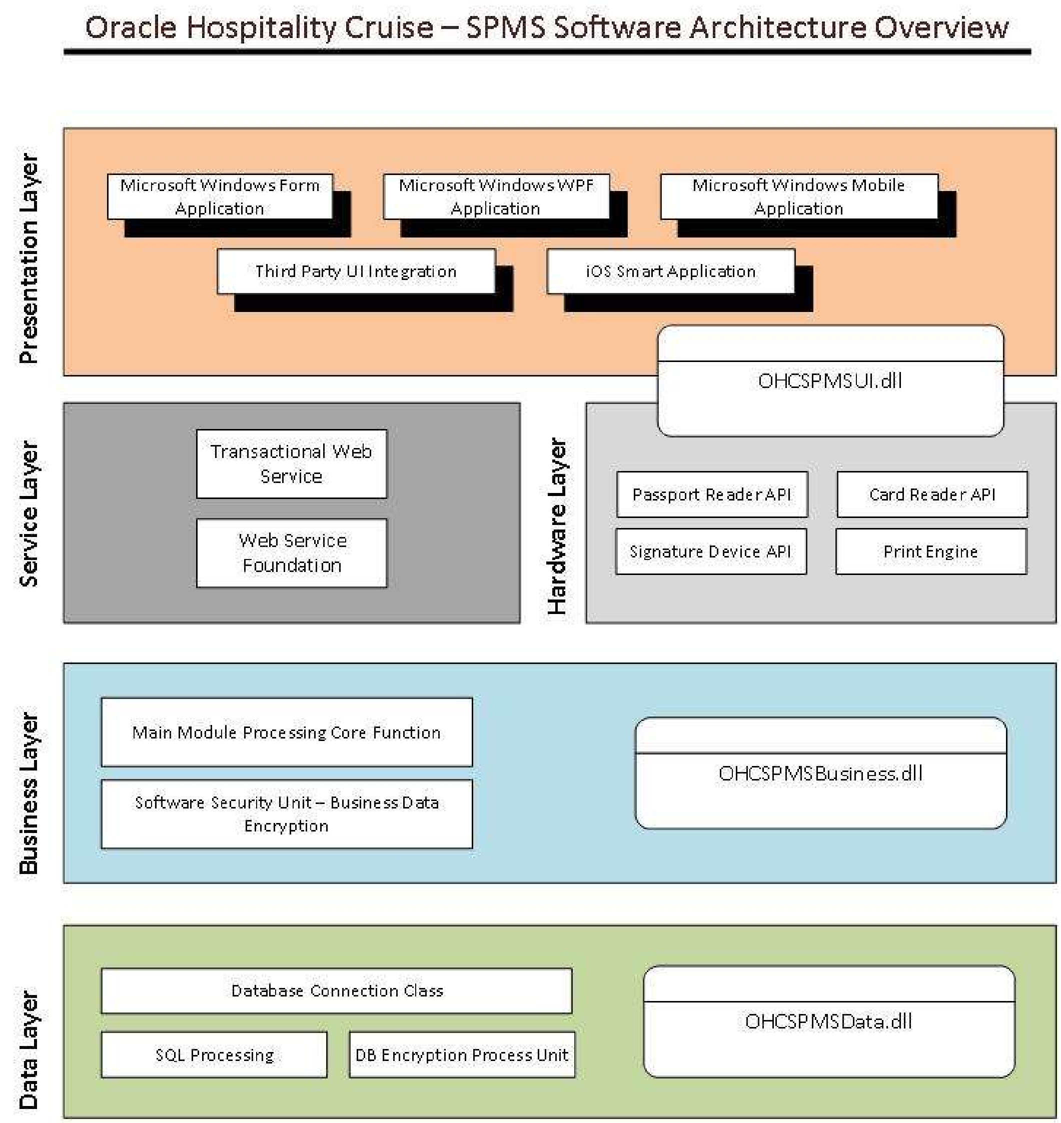

Oracle Hospitality Cruise – SPMS Software Architecture Overview
Presentation Layer
Microsoft Windows Form Application
Microsoft Windows WPF Application
Microsoft Windows Mobile Application
Third Party UI Integration
iOS Smart Application
OHCSPMSUI.dll
Service Layer
Transactional Web Service
Web Service Foundation
Hardware Layer
Passport Reader API
Card Reader API
Signature Device API
Print Engine
Business Layer
Main Module Processing Core Function
Software Security Unit – Business Data Encryption
OHCSPMSBusiness.dll
Data Layer
Database Connection Class
SQL Processing
DB Encryption Process Unit
OHCSPMSData.dll

Figure 2 - Shipboard Property Management System Detailed Software 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.

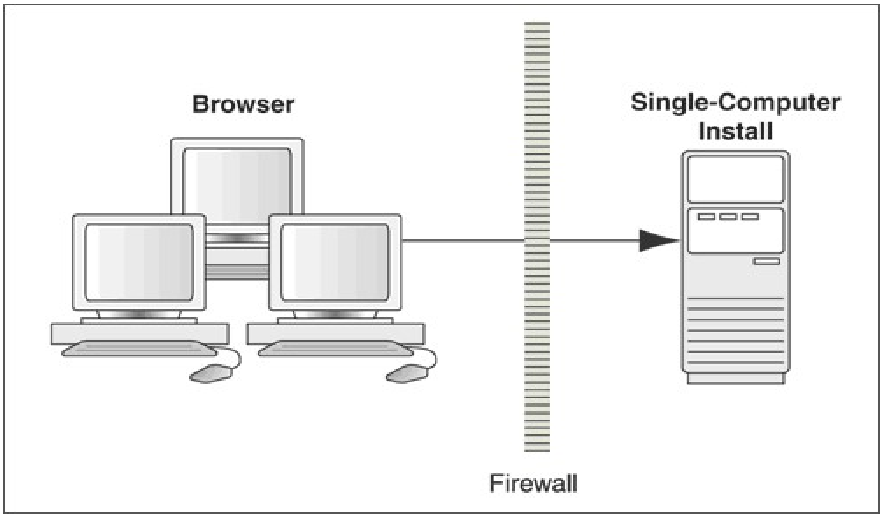


Figure 2-2 - Single Computer Deployment Architecture

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*.

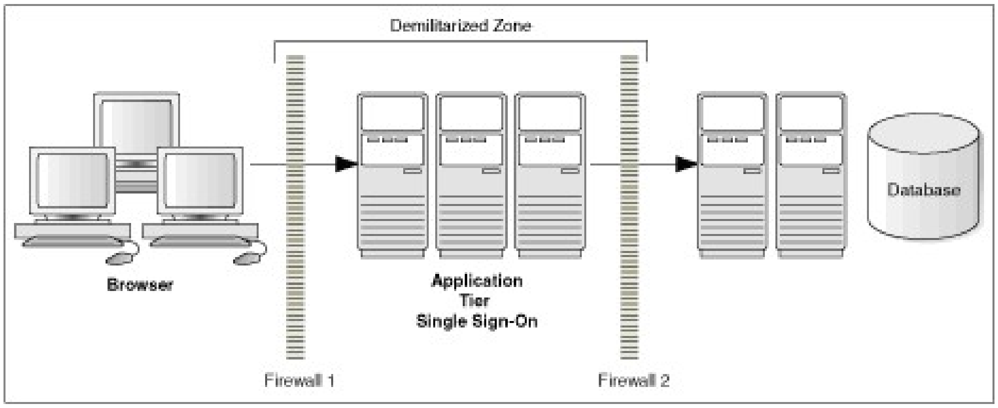


Figure 2-3 - Traditional DMZ View

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.

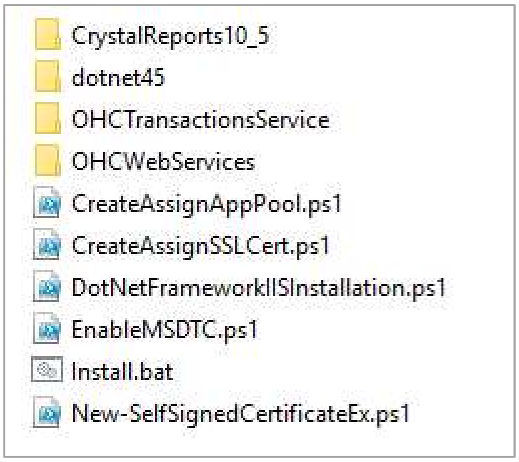
- For Microsoft Windows 10 user, ensure the **Microsoft .NET Framework 2 and 3.5** is turned on in Window Features before installing Oracle Full Client and **OHC_SPMS_V8SETUP.exe**
- For Microsoft Windows 7 user, ensure the **Microsoft .NET Framework 4.5** is installed, or download a copy of the installation 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 **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.

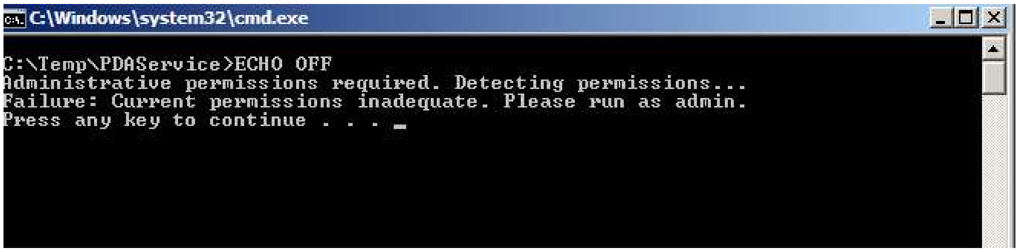


CrystalReports10_5
dotnet45
OHCTransactionsService
OHCWebServices
CreateAssignAppPool.ps1
CreateAssignSSLCert.ps1
DotNetFrameworkIISInstallation.ps1
EnableMSDTC.ps1
Install.bat
New-SelfSignedCertificateEx.ps1

Figure 3-1 - Webservices Files

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

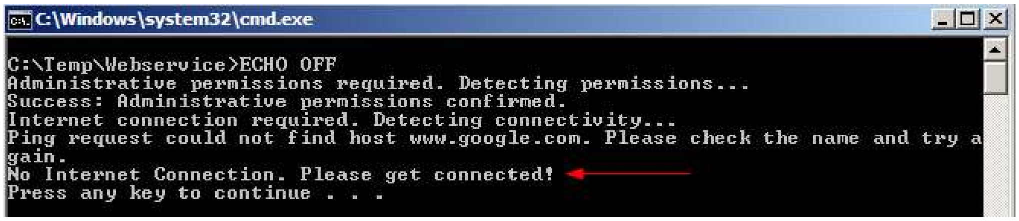
   If the user tries to run the batch file without an Administrator login, the system prompts a failure as shown below.



```
C:\Temp\PDAService>ECHO OFF
Administrative permissions required. Detecting permissions...
Failure: Current permissions inadequate. Please run as admin.
Press any key to continue . . . _
```

Figure 3-2 – Installation Failure Prompt

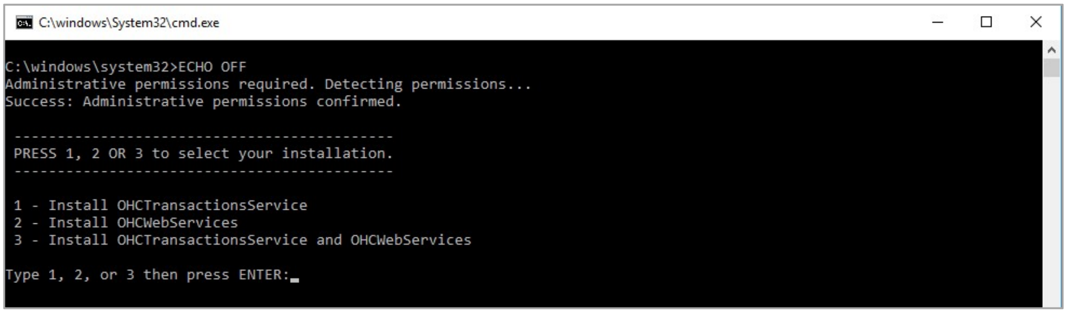
The System then scans for an Internet connection and proceeds with the installation when the Internet connection is established. Otherwise, the installation will abort.



```
C:\Temp\Webservice>ECHO OFF
Administrative permissions required. Detecting permissions...
Success: Administrative permissions confirmed.
Internet connection required. Detecting connectivity...
Ping request could not find host www.google.com. Please check the name and try a
gain.
No Internet Connection. Please get connected!
Press any key to continue . . .
```

Figure 3-3 - Internet Connection Prompt

When an Internet connection is detected, the system will prompt a selection menu.



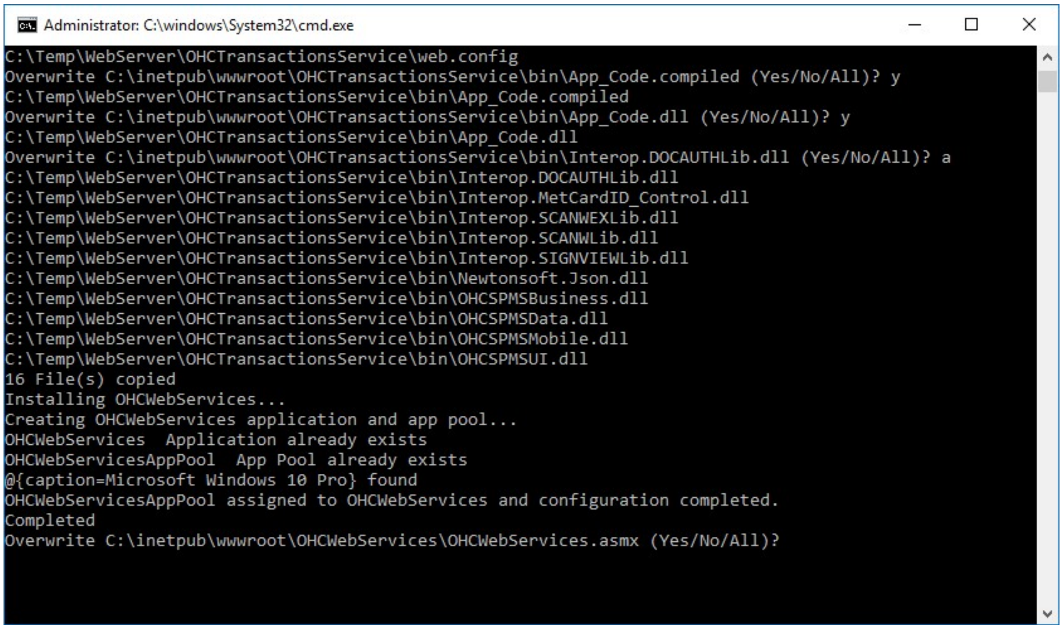
```
C:\windows\system32>ECHO OFF
Administrative permissions required. Detecting permissions...
Success: Administrative permissions confirmed.

 --------------------------------------------
 PRESS 1, 2 OR 3 to select your installation.
 --------------------------------------------

 1 - Install OHCTransactionsService
 2 - Install OHCWebServices
 3 - Install OHCTransactionsService and OHCWebServices

Type 1, 2, or 3 then press ENTER:_
```

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.

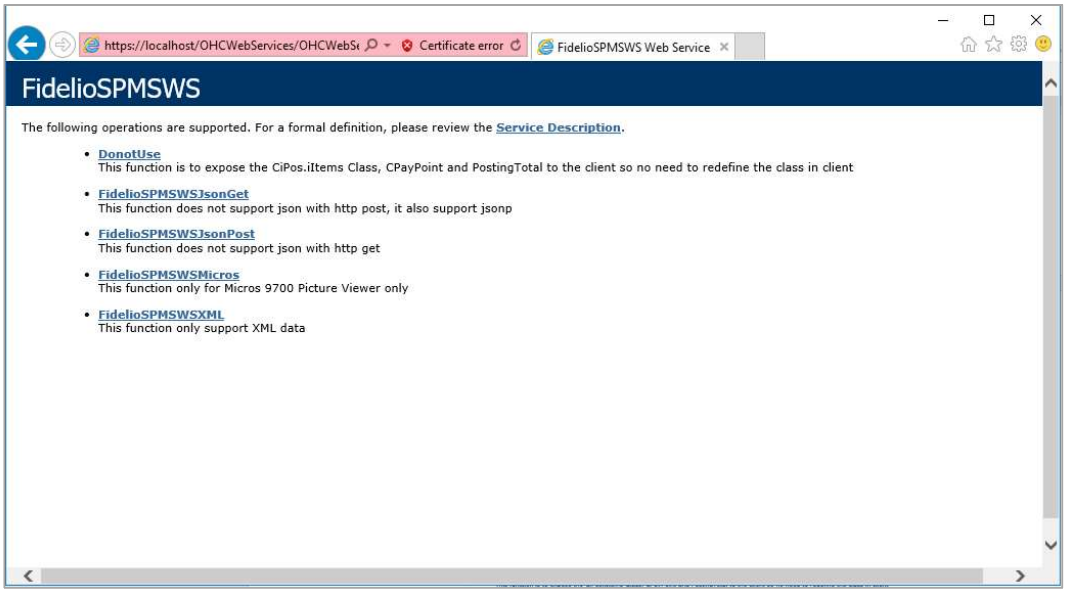


```
C:\Temp\WebServer\OHCTransactionsService\web.config
Overwrite C:\inetpub\wwwroot\OHCTransactionsService\bin\App_Code.compiled (Yes/No/All)? y
C:\Temp\WebServer\OHCTransactionsService\bin\App_Code.compiled
Overwrite C:\inetpub\wwwroot\OHCTransactionsService\bin\App_Code.dll (Yes/No/All)? y
C:\Temp\WebServer\OHCTransactionsService\bin\App_Code.dll
Overwrite C:\inetpub\wwwroot\OHCTransactionsService\bin\Interop.DOCAUTHLib.dll (Yes/No/All)? a
C:\Temp\WebServer\OHCTransactionsService\bin\Interop.DOCAUTHLib.dll
C:\Temp\WebServer\OHCTransactionsService\bin\Interop.MetCardID_Control.dll
C:\Temp\WebServer\OHCTransactionsService\bin\Interop.SCANWEXLib.dll
C:\Temp\WebServer\OHCTransactionsService\bin\Interop.SCANWLib.dll
C:\Temp\WebServer\OHCTransactionsService\bin\Interop.SIGNVIEWLib.dll
C:\Temp\WebServer\OHCTransactionsService\bin\Newtonsoft.Json.dll
C:\Temp\WebServer\OHCTransactionsService\bin\OHCSPMSBusiness.dll
C:\Temp\WebServer\OHCTransactionsService\bin\OHCSPMSData.dll
C:\Temp\WebServer\OHCTransactionsService\bin\OHCSPMSMobile.dll
C:\Temp\WebServer\OHCTransactionsService\bin\OHCSPMSUI.dll
16 File(s) copied
Installing OHCWebServices...
Creating OHCWebServices application and app pool...
OHCWebServices  Application already exists
OHCWebServicesAppPool  App Pool already exists
@{caption=Microsoft Windows 10 Pro} found
OHCWebServicesAppPool assigned to OHCWebServices and configuration completed.
Completed
Overwrite C:\inetpub\wwwroot\OHCWebServices\OHCWebServices.asmx (Yes/No/All)?
```

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.



https://localhost/OHCWebServices/OHCWebS
Certificate error
FidelioSPMSWS Web Service

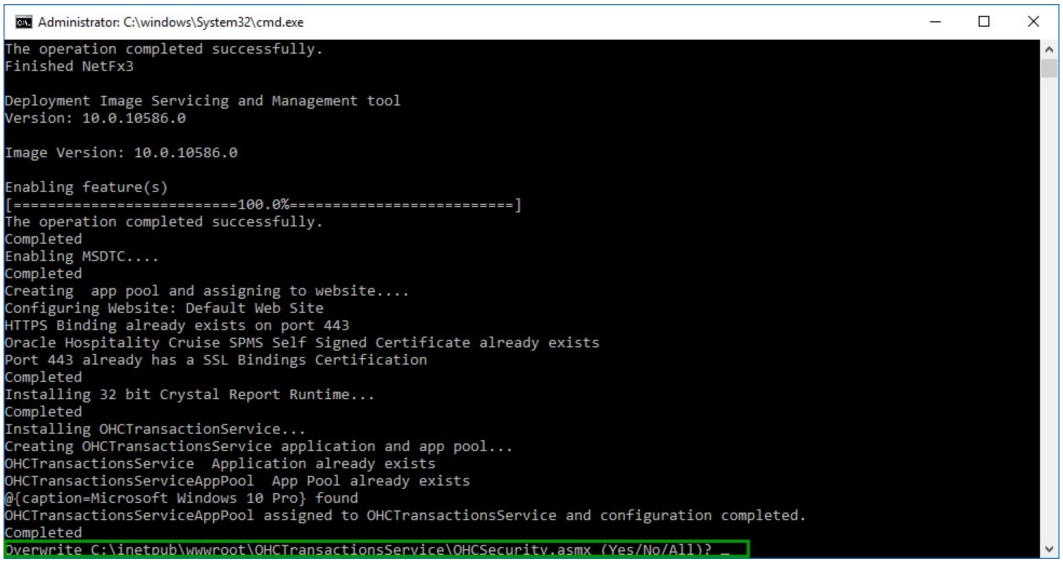
FidelioSPMSWS

The following operations are supported. For a formal definition, please review the Service Description.

- DonotUse
  This function is to expose the CiPos.iItems Class, CPayPoint and PostingTotal to the client so no need to redefine the class in client
- FidelioSPMSWSJsonGet
  This function does not support json with http post, it also support jsonp
- FidelioSPMSWSJsonPost
  This function does not support json with http get
- FidelioSPMSWSMicros
  This function only for Micros 9700 Picture Viewer only
- FidelioSPMSWSXML
  This function only support XML data

Figure 3-6 - Verification of 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.



```
The operation completed successfully.
Finished NetFx3

Deployment Image Servicing and Management tool
Version: 10.0.10586.0

Image Version: 10.0.10586.0

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
Completed
Enabling MSDTC....
Completed
Creating  app pool and assigning to website....
Configuring Website: Default Web Site
HTTPS Binding already exists on port 443
Oracle Hospitality Cruise SPMS Self Signed Certificate already exists
Port 443 already has a SSL Bindings Certification
Completed
Installing 32 bit Crystal Report Runtime...
Completed
Installing OHCTransactionService...
Creating OHCTransactionsService application and app pool...
OHCTransactionsService  Application already exists
OHCTransactionsServiceAppPool  App Pool already exists
@{caption=Microsoft Windows 10 Pro} found
OHCTransactionsServiceAppPool assigned to OHCTransactionsService and configuration completed.
Completed
Overwrite C:\inetpub\wwwroot\OHCTransactionsService\OHCSecurity.asmx (Yes/No/All)? _
```

Figure 3-7 - Upgrading WebServices

Establishing a connection

Web Service Connection

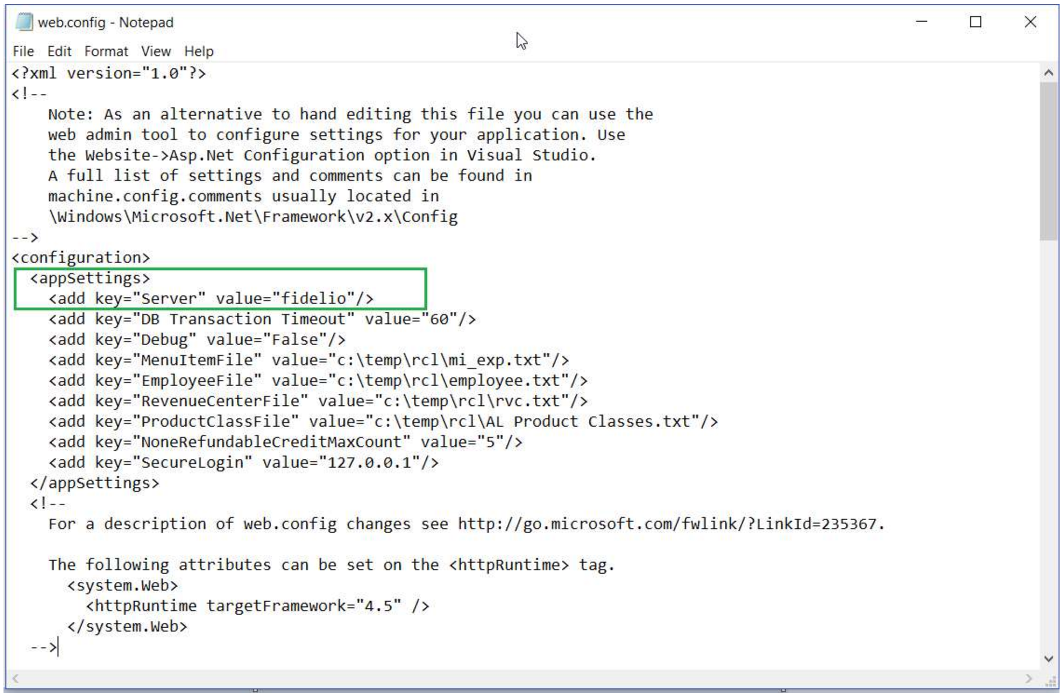
For Simphony users:

- 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>`.

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

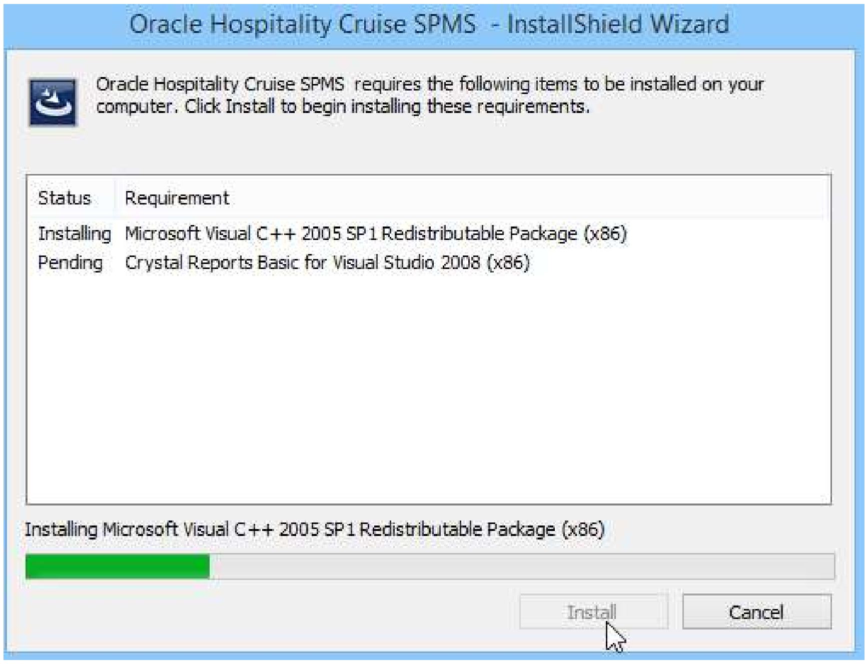


```
<?xml version="1.0"?>
<!--
    Note: As an alternative to hand editing this file you can use the
    web admin tool to configure settings for your application. Use
    the Website->Asp.Net Configuration option in Visual Studio.
    A full list of settings and comments can be found in
    machine.config.comments usually located in
    \Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration>
  <appSettings>
    <add key="Server" value="fidelio"/>
    <add key="DB Transaction Timeout" value="60"/>
    <add key="Debug" value="False"/>
    <add key="MenuItemFile" value="c:\temp\rcl\mi_exp.txt"/>
    <add key="EmployeeFile" value="c:\temp\rcl\employee.txt"/>
    <add key="RevenueCenterFile" value="c:\temp\rcl\rvc.txt"/>
    <add key="ProductClassFile" value="c:\temp\rcl\AL Product Classes.txt"/>
    <add key="NoneRefundableCreditMaxCount" value="5"/>
    <add key="SecureLogin" value="127.0.0.1"/>
  </appSettings>
  <!--
    For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

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

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.


Oracle Hospitality Cruise SPMS - InstallShield Wizard

Oracle Hospitality Cruise SPMS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Installing	Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)
Pending	Crystal Reports Basic for Visual Studio 2008 (x86)

Installing Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)

Figure 3-9 – Oracle Hospitality Cruise SPMS Installation

8. Click **Install** and follow the installation wizard to complete the setup.
9. After the installation completes, ensure the database connection is established by using NetManager.exe to check the connection.
10. Navigate to Windows Control Panel, Programs and Feature and uninstall **FCruiseSetup730** from the system.
11. Launch Notepad.exe and create a *new* text file with one of this content:
    - IP Address of IIS Server
    - IIS Server Name
12. 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
    - OHCSPMSMobile.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.

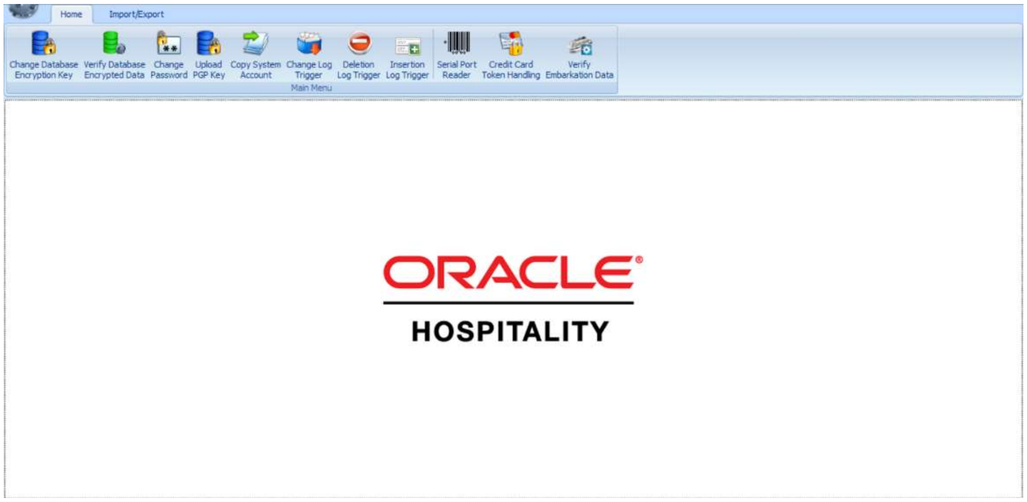


Figure 3-10 - OHC Tools Main Screen.

3. In the Encryption Key Manager window, enter the **Passphrase1** and **Passphrase 2, Old Fidelio password, Fidelio Password** and **Confirm** password.

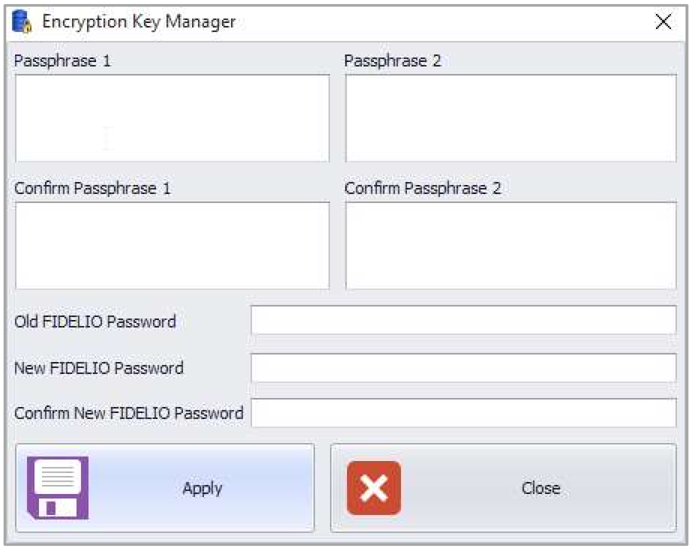


Figure 3-11 - Encryption Passphrase

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
     - OHCSPMSUI.dll
     - OHCWebSockets.dll
   - REGASM Files
     - CRUFLFC.dll
     - OHCSPMSData.dll
     - OHCSPMSBusiness.dll
     - OHCSPMSMobile.dll
     - OHCSPMSUtils.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)

Turn on DEP if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning off Auto Play

Turn off Autoplay if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Remote Assistance

Turn off Remote Assistance if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

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.

4 Shipboard Property Management System Security

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).

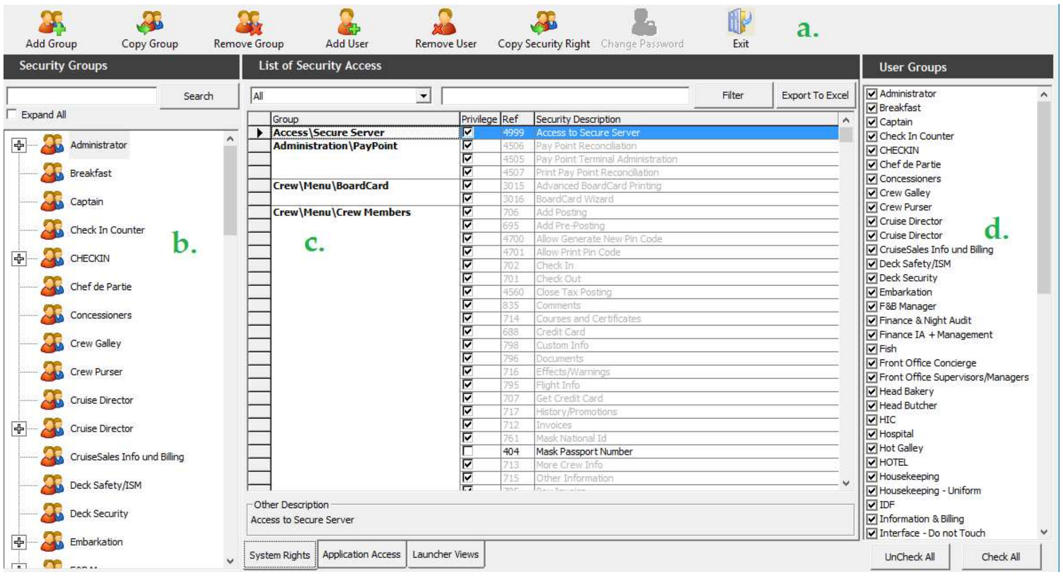
The Oracle Hospitality Cruise Launch Panel is a control panel to SPMS programs and User Security Management.

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.



Group	Privilege	Ref	Security Description
Access\Secure Server	☑	4999	Access to Secure Server
Administration\PayPoint	☑	4506	Pay Point Reconciliation
	☑	4505	Pay Point Terminal Administration
	☑	4507	Print Pay Point Reconciliation
Crew\Menu\BoardCard	☑	3015	Advanced BoardCard Printing
	☑	3016	BoardCard Wizard
Crew\Menu\Crew Members	☑	706	Add Posting
	☑	695	Add Pre-Posting
	☑	4700	Allow Generate New Pin Code
	☑	4701	Allow Print Pin Code
	☑	702	Check In
	☑	701	Check Out
	☑	4560	Close Tax Posting
	☑	835	Comments
	☑	714	Courses and Certificates
	☑	688	Credit Card
	☑	798	Custom Info
	☑	796	Documents
	☑	716	Effects/Warnings
	☑	795	Flight Info
	☑	707	Get Credit Card
	☑	717	History/Promotions
	☑	712	Invoices
	☑	761	Mask National Id
	□	404	Mask Passport Number
	☑	713	More Crew Info
	☑	715	Other Information

Other Description
Access to Secure Server

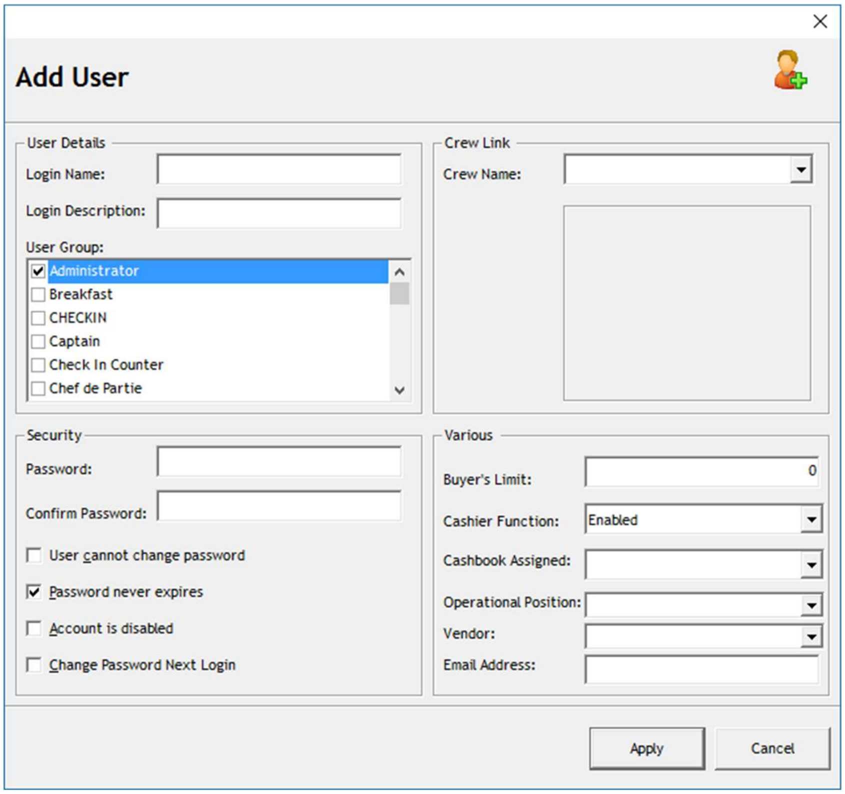
☑ Administrator
☑ Breakfast
☑ Captain
☑ Check In Counter
☑ CHECKIN
☑ Chef de Partie
☑ Concessioners
☑ Crew Galley
☑ Crew Purser
☑ Cruise Director
☑ Cruise Director
☑ CruiseSales Info und Billing
☑ Deck Safety/ISM
☑ Deck Security
☑ Embarkation
☑ F&B Manager
☑ Finance & Night Audit
☑ Finance IA + Management
☑ Fish
☑ Front Office Concierge
☑ Front Office Supervisors/Managers
☑ Head Bakery
☑ Head Butcher
☑ HIC
☑ Hospital
☑ Hot Galley
☑ HOTEL
☑ Housekeeping
☑ Housekeeping - Uniform
☑ IDF
☑ Information & Billing
☑ Interface - Do not Touch

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

User Details

Login Name:

Login Description:

User Group:

☑ Administrator
□ Breakfast
□ CHECKIN
□ Captain
□ Check In Counter
□ Chef de Partie

Crew Link

Crew Name:

Security

Password:

Confirm Password:

□ User cannot change password
☑ Password never expires
□ Account is disabled
□ Change Password Next Login

Various

Buyer's Limit: 0

Cashier Function: Enabled

Cashbook Assigned:

Operational Position:

Vendor:

Email Address:

Figure 4-2 - Add User Screen

Table 4-1- Field/Description Table

Field	Description
Login Name	Login ID used in SPMS applications.
Login Description	User Name

Field	Description
User Group	Group Access Level
Password	User Password
Crew Link	Link to Crew Profile
Buyer's Limit	Maximum spend amount allowed for goods purchases from MMS module.
Cashier Function	Enable/Disable Cashier Function.
Cashbook Assigned	Cashbook assignment
Operational Position	Operational Position user is link to.
Vendor	A user by iCrew WebServices to retrieve an excursion.
Email Address	Email address of the user.

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

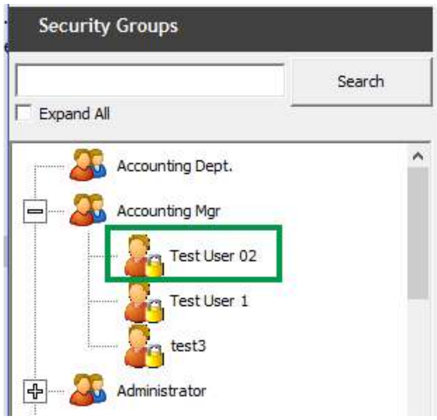
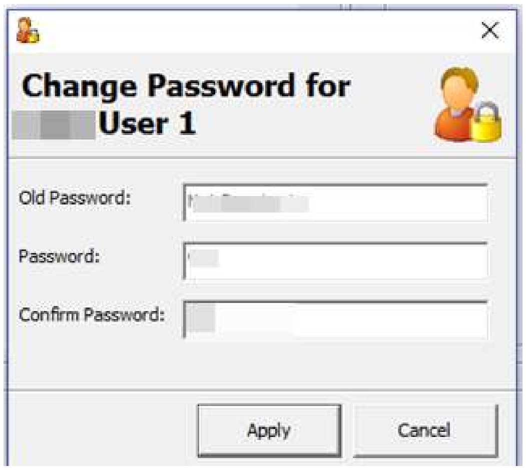


Figure 4-3 – User Security – Add user – Security Groups

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.



Change Password for [redacted] User 1

Old Password: [redacted]

Password: [redacted]

Confirm Password: [redacted]

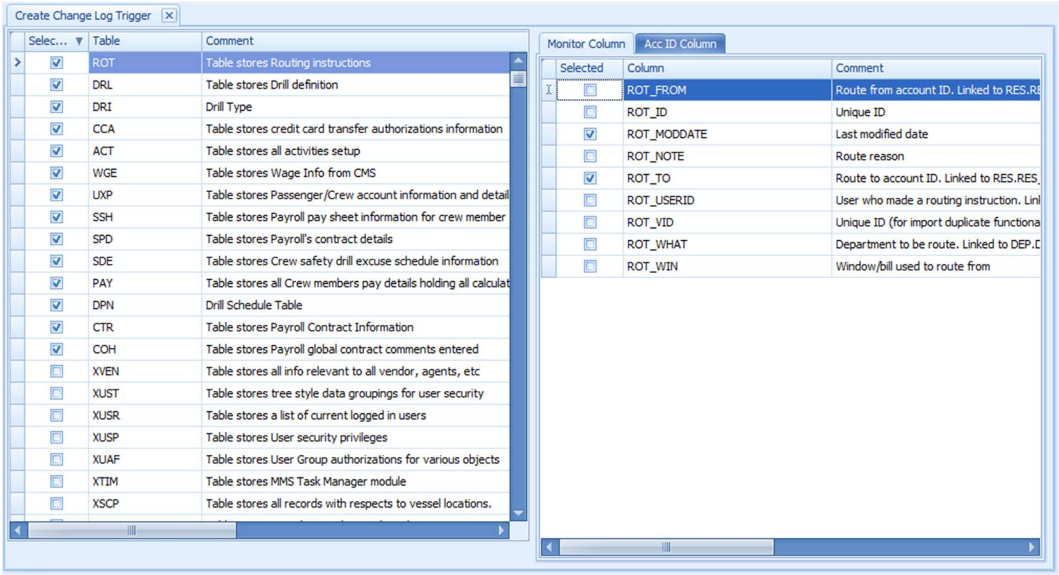
Figure 4-4 – User Security – Change Password

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.



Selec...	Table	Comment
☑	ROT	Table stores Routing instructions
☑	DRL	Table stores Drill definition
☑	DRI	Drill Type
☑	CCA	Table stores credit card transfer authorizations information
☑	ACT	Table stores all activities setup
☑	WGE	Table stores Wage Info from CMS
☑	UXP	Table stores Passenger/Crew account information and detail
☑	SSH	Table stores Payroll pay sheet information for crew member
☑	SPD	Table stores Payroll's contract details
☑	SDE	Table stores Crew safety drill excuse schedule information
☑	PAY	Table stores all Crew members pay details holding all calculat
☑	DPN	Drill Schedule Table
☑	CTR	Table stores Payroll Contract Information
☑	COH	Table stores Payroll global contract comments entered
□	XVEN	Table stores all info relevant to all vendor, agents, etc
□	XUST	Table stores tree style data groupings for user security
□	XUSR	Table stores a list of current logged in users
□	XUSP	Table stores User security privileges
□	XUAF	Table stores User Group authorizations for various objects
□	XTIM	Table stores MMS Task Manager module
□	XSCP	Table stores all records with respects to vessel locations.

Selected	Column	Comment
□	ROT_FROM	Route from account ID. Linked to RES.RE
□	ROT_ID	Unique ID
☑	ROT_MODDATE	Last modified date
□	ROT_NOTE	Route reason
☑	ROT_TO	Route to account ID. Linked to RES.RES_
□	ROT_USERID	User who made a routing instruction. Linl
□	ROT_VID	Unique ID (for import duplicate functiona
□	ROT_WHAT	Department to be route. Linked to DEP.D
□	ROT_WIN	Window/bill used to route from

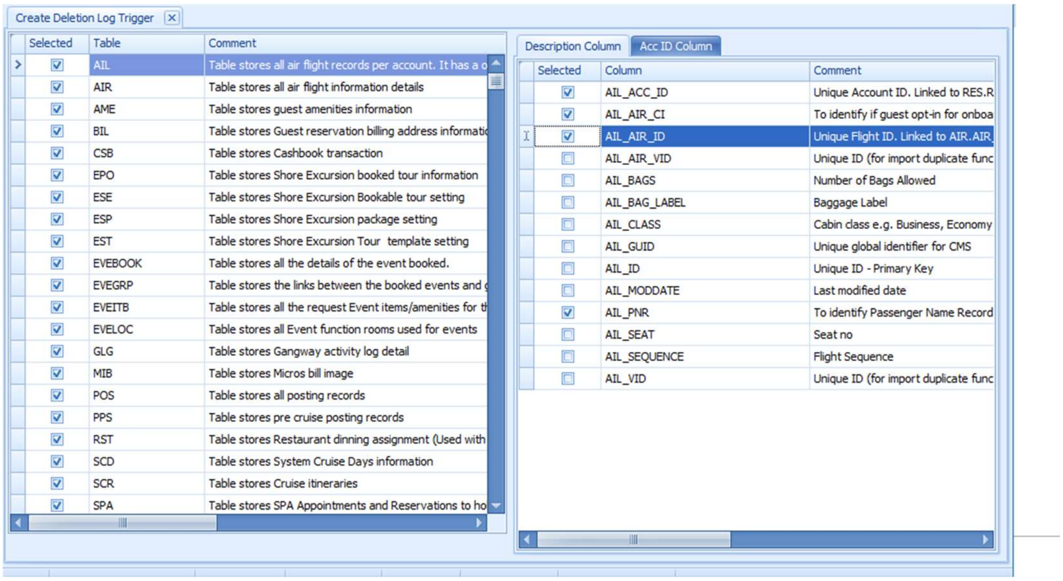
Figure 4-5 - Change Log Trigger

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.



Selected	Table	Comment
☑	AIL	Table stores all air flight records per account. It has a o
☑	AIR	Table stores all air flight information details
☑	AME	Table stores guest amenities information
☑	BIL	Table stores Guest reservation billing address informatic
☑	CSB	Table stores Cashbook transaction
☑	EPO	Table stores Shore Excursion booked tour information
☑	ESE	Table stores Shore Excursion Bookable tour setting
☑	ESP	Table stores Shore Excursion package setting
☑	EST	Table stores Shore Excursion Tour template setting
☑	EVEBOOK	Table stores all the details of the event booked.
☑	EVEGRP	Table stores the links between the booked events and g
☑	EVEITB	Table stores all the request Event items/amenities for th
☑	EVELOC	Table stores all Event function rooms used for events
☑	GLG	Table stores Gangway activity log detail
☑	MIB	Table stores Micros bill image
☑	POS	Table stores all posting records
☑	PPS	Table stores pre cruise posting records
☑	RST	Table stores Restaurant dinning assignment (Used with
☑	SCD	Table stores System Cruise Days information
☑	SCR	Table stores Cruise itineraries
☑	SPA	Table stores SPA Appointments and Reservations to ho

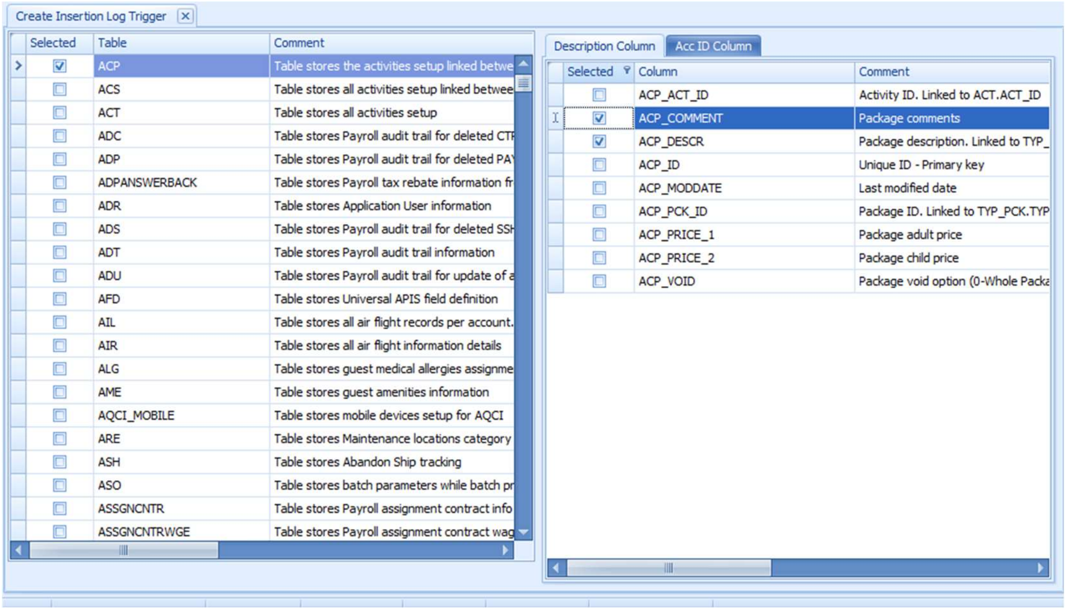
Selected	Column	Comment
☑	AIL_ACC_ID	Unique Account ID. Linked to RES.R
☑	AIL_AIR_CI	To identify if guest opt-in for onboa
☑	AIL_AIR_ID	Unique Flight ID. Linked to AIR.AIR_
☐	AIL_AIR_VID	Unique ID (for import duplicate func
☐	AIL_BAGS	Number of Bags Allowed
☐	AIL_BAG_LABEL	Baggage Label
☐	AIL_CLASS	Cabin class e.g. Business, Economy
☐	AIL_GUID	Unique global identifier for CMS
☐	AIL_ID	Unique ID - Primary Key
☐	AIL_MODDATE	Last modified date
☑	AIL_PNR	To identify Passenger Name Record
☐	AIL_SEAT	Seat no
☐	AIL_SEQUENCE	Flight Sequence
☐	AIL_VID	Unique ID (for import duplicate func

Figure 4-6 - Deletion Log Trigger

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.



Selected	Table	Comment
☑	ACP	Table stores the activities setup linked betwe
□	ACS	Table stores all activities setup linked betwee
□	ACT	Table stores all activities setup
□	ADC	Table stores Payroll audit trail for deleted CTI
□	ADP	Table stores Payroll audit trail for deleted PA'
□	ADPANSWERBACK	Table stores Payroll tax rebate information fr
□	ADR	Table stores Application User information
□	ADS	Table stores Payroll audit trail for deleted SSI
□	ADT	Table stores Payroll audit trail information
□	ADU	Table stores Payroll audit trail for update of a
□	AFD	Table stores Universal APIS field definition
□	AIL	Table stores all air flight records per account.
□	AIR	Table stores all air flight information details
□	ALG	Table stores guest medical allergies assignme
□	AME	Table stores guest amenities information
□	AQCI_MOBILE	Table stores mobile devices setup for AQCI
□	ARE	Table stores Maintenance locations category
□	ASH	Table stores Abandon Ship tracking
□	ASO	Table stores batch parameters while batch pr
□	ASSGNCNTR	Table stores Payroll assignment contract info
□	ASSGNCNTRWGE	Table stores Payroll assignment contract wag

Selected	Column	Comment
□	ACP_ACT_ID	Activity ID. Linked to ACT.ACT_ID
☑	ACP_COMMENT	Package comments
☑	ACP_DESCR	Package description. Linked to TYP_
□	ACP_ID	Unique ID - Primary key
□	ACP_MODDATE	Last modified date
□	ACP_PCK_ID	Package ID. Linked to TYP_PCK.TYP
□	ACP_PRICE_1	Package adult price
□	ACP_PRICE_2	Package child price
□	ACP_VOID	Package void option (0-Whole Packa

Figure 4-7 - Insertion Log Trigger

1. At the OHC Tools window, select **Insertion Log Trigger** from the ribbon bar.
2. 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`.
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 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.

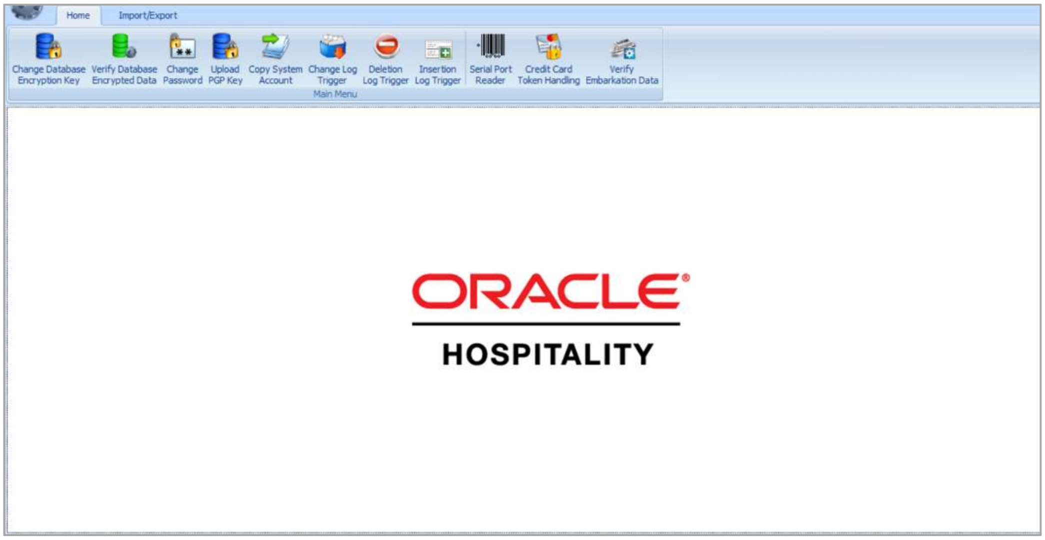


Figure 4-8 - OHC Tools Main Screen

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.

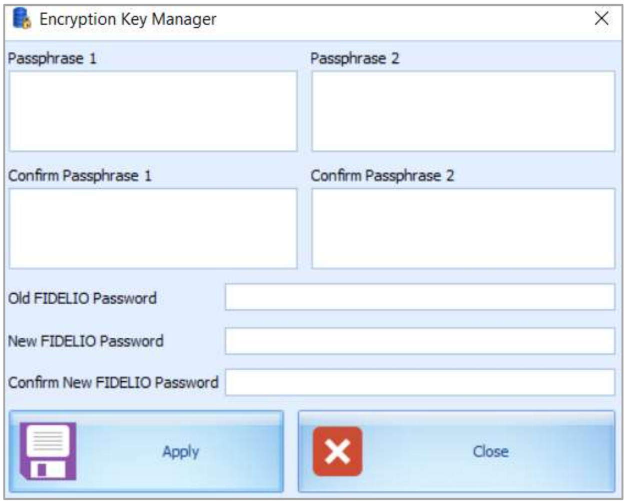
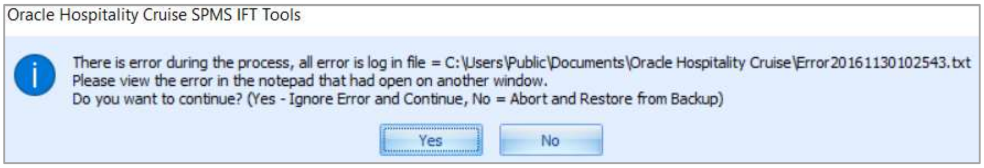


Figure 4-9 - Encryption Passphrase

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.



Oracle Hospitality Cruise SPMS IFT Tools

There is error during the process, all error is log in file = C:\Users\Public\Documents\Oracle Hospitality Cruise\Error20161130102543.txt
Please view the error in the notepad that had open on another window.
Do you want to continue? (Yes - Ignore Error and Continue, No = Abort and Restore from Backup)

Figure 4-10 - Error Prompt

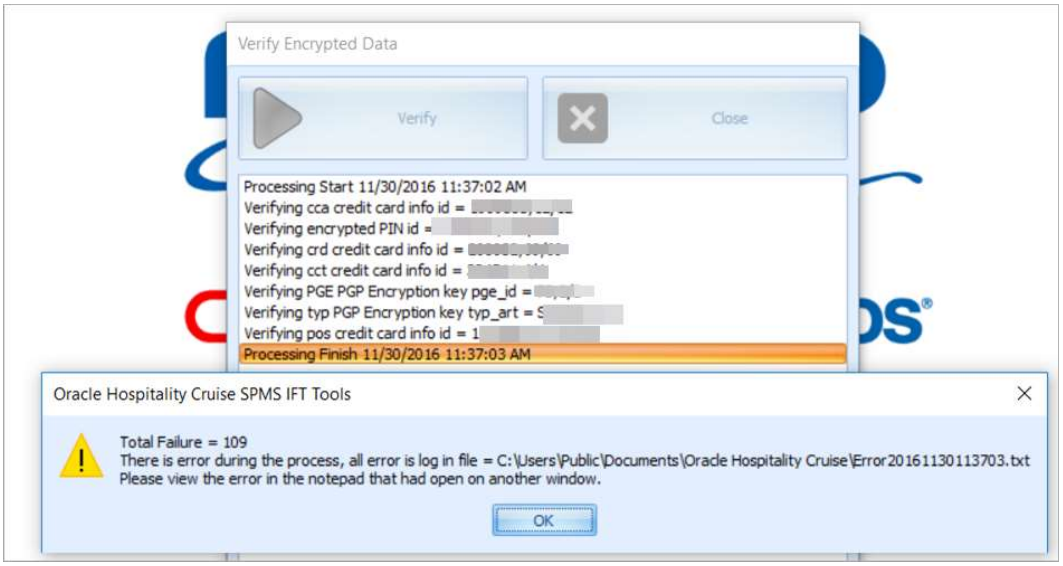
4. At the prompt, choose to **Yes** to continue replacing the encryption key or **<u>No</u>** to roll back the process by restoring the backup. The Passphrase is saved in *OHCSecurity.par* with one-year validity from the date of encryption.

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.



```
Processing Start 11/30/2016 11:37:02 AM
Verifying cca credit card info id = [redacted]
Verifying encrypted PIN id = [redacted]
Verifying crd credit card info id = [redacted]
Verifying cct credit card info id = [redacted]
Verifying PGE PGP Encryption key pge_id = [redacted]
Verifying typ PGP Encryption key typ_art = [redacted]
Verifying pos credit card info id = [redacted]
Processing Finish 11/30/2016 11:37:03 AM
```

Oracle Hospitality Cruise SPMS IFT Tools

Total Failure = 109
There is error during the process, all error is log in file = C:\Users\Public\Documents\Oracle Hospitality Cruise\Error20161130113703.txt
Please view the error in the notepad that had open on another window.

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.

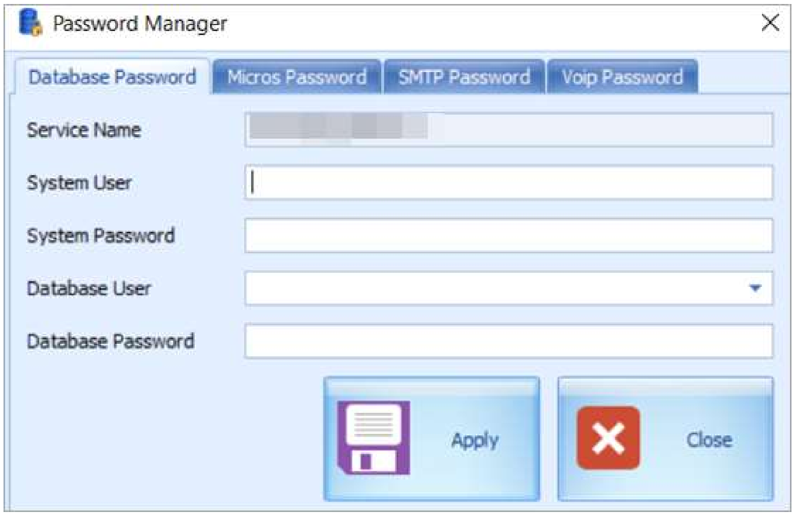


Figure 4-12 - Change Password Window

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

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