

**Oracle® Hospitality Cruise Shipboard  
Property Management System**

Tools User Guide

Release 8.0

**E84869-03**

December 2019

---

Copyright © 1995, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

<b>Figures</b> .....	<b>4</b>
<b>Preface</b> .....	<b>5</b>
Audience .....	5
Customer Support.....	5
Documentation .....	5
Revision History.....	5
<b>OHC Tools</b> .....	<b>6</b>
Creating Database Encryption Key .....	6
Creating Database Encryption Key for Upgrade.....	7
Changing Database Encryption Key .....	10
Creating an Encryption Passphrase .....	10
Verifying The Encrypted Database Data .....	11
Verifying Encrypted Data.....	11
Changing Password.....	12
Uploading PGP Key.....	13
Copying System Account.....	13
Changing Log Trigger .....	14
Deleting Log Trigger .....	14
Inserting Log Trigger.....	14
Serial Port Reader.....	15
Credit Card Token Handling .....	15
Verifying Embarkation Data .....	16
Exporting Database.....	17
Importing Database .....	18
Exporting Safety Setup.....	19
Importing Safety Setup .....	19
Exporting Package Template.....	20
Importing Package Template .....	21
Importing Barcode for Symphony .....	21

---

---

# Figures

Figure 1- Functions in Tools Home Tab .....	6
Figure 2 - Function in Tools Import/Export Tab .....	6
Figure 3 - Update DPAPI Key .....	7
Figure 4 - OHC Tools Main Screen before DB Upgrade .....	8
Figure 5 - Encryption Passphrase.....	8
Figure 6 - Encryption Passphrase.....	10
Figure 7 - DMP Password Form.....	11
Figure 8 - Verify Database Encrypted Data .....	12
Figure 9 - Change Password Window.....	12
Figure 10 - PGP Key Uploader .....	13
Figure 11 - Copy System Account.....	14
Figure 12 - OHC Credit Card Token Handling.....	16
Figure 13 - Sample Non-ASCII Records Less Than 18 Characters .....	17
Figure 14 - Sample Non-ASCII Code Value More Than 18 Characters .....	17
Figure 15 - DMP Password .....	17
Figure 16 - Import Database .....	18
Figure 17 - DMP File Password.....	18
Figure 18 - Import Database - Table Excluded/Does Not Exist .....	18
Figure 19 - Export Safety Setup .....	19
Figure 20 - Import Safety Setup.....	19
Figure 21 - Failed Import Safety Setup Message.....	20
Figure 22 - Export Package Template .....	20
Figure 23 - Import Package Template .....	21
Figure 24 - Symphony Barcode Import .....	22

---

---

# Preface

The Tools is a program that manages data security in Oracle Hospitality Cruise Shipboard Management System (SPMS) such as securing credit card data with an encryption key, changing of database password, export/import database with secure password and others.

## Audience

This document is intended for application specialist and end users of Oracle Hospitality Cruise 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

Date	Description of Change
March 2017	<ul style="list-style-type: none"><li>• Initial publication</li></ul>
May 2018	<ul style="list-style-type: none"><li>• Added Transparent Data Encryption process.</li></ul>
December 2019	<ul style="list-style-type: none"><li>• Added steps to create Database Encryption Key</li></ul>

---

---

# OHC Tools

The Tools application manages the data security, credit card data encryption, database password change and has an added database import/export functionality.



Figure 1- Functions in Tools Home Tab



Figure 2 - Function in Tools Import/Export Tab

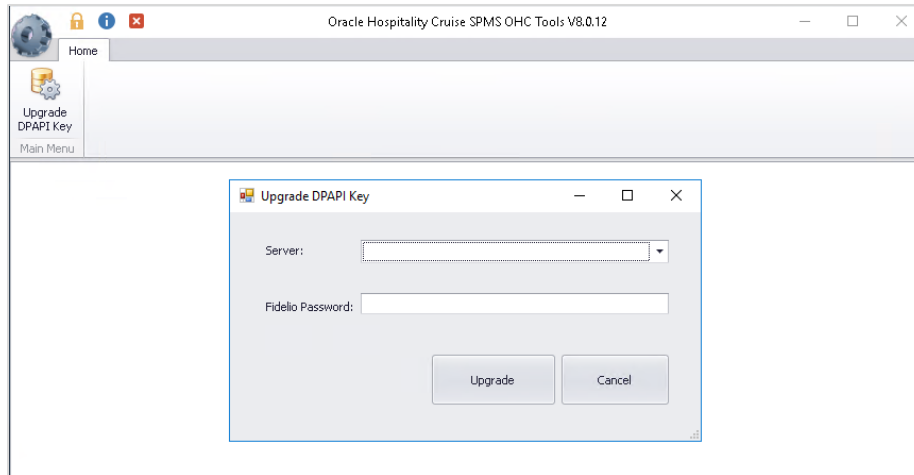
## Creating Database Encryption Key

 **NOTE:**

This section is mandatory step to be followed to successfully login into the application.

From version 8.0.12 onwards, you are required to create a shortcut for OHC Tools.exe and insert **"/m"** in **Properties, Target** field using below steps

1. Login to the Client PC as a standard user.
2. Navigate to the Program Files folder of the application and create a desktop shortcut for OHC Tools.exe.
3. Go to **Properties, Target** field of the shortcut and insert **"/m"** at the end of the string. For example, "C:\Program Files (x86)\Oracle Hospitality Cruise\OHC Tools.exe" /m.
4. When running **OHC Tools.exe** from the shortcut, the system will display the below screen, enabling you to update the DPAPI key and create a new OHC Security.par file.

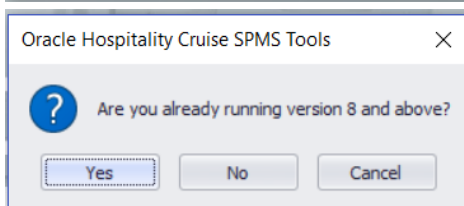
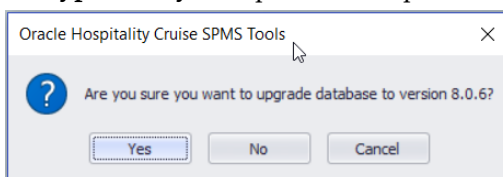


**Figure 3 - Update DPAPI Key**

5. Click on **Upgrade DPAPI Key**.
6. At the Upgrade DPAPI Key window, input the **DB Server Data Source name** , **schema password** and click **Upgrade** to proceed. The program verifies your database password and creates new OHC Security.par.

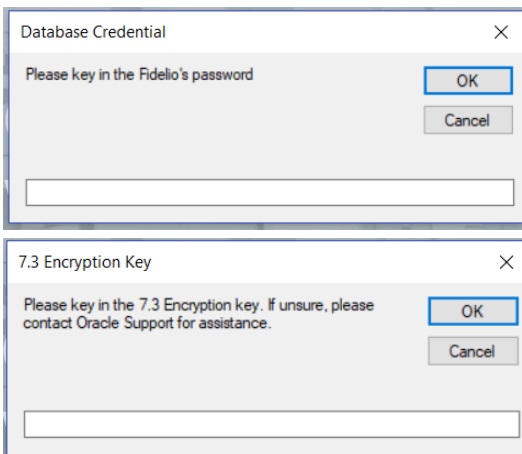
## Creating Database Encryption Key for Upgrade

1. Login to the Client PC as a standard user.
2. From version 8.0.6 onwards, you are required to create a shortcut for OHC Tools.exe and insert **"/u"** in the **Properties, Target** field by right-clicking the shortcut and select **Properties**. For example, "C:\Program Files (x86)\Oracle Hospitality Cruise\OHC Tools.exe" /u.
3. When running **OHC Tools.exe** from version 8.0.6 onwards, the system will prompt "Are you sure you want to upgrade the version to 8.0.6?". Select **Yes** to proceed with the upgrade and you will be prompt to insert a **Database Password** followed by an **Encryption key** as explicate in step 4.



4. At the Database Credential prompt, input the old database password and click **OK** to proceed. The program verifies your database and proceed when the version is below 8.0 and prompt for the 7.30 **Encryption Key** to be entered.
5. Enter the key in the field and click **OK**.

If you are already on version 8.0, the system does not permit you to upgrade and prompt you a **Login** screen instead.

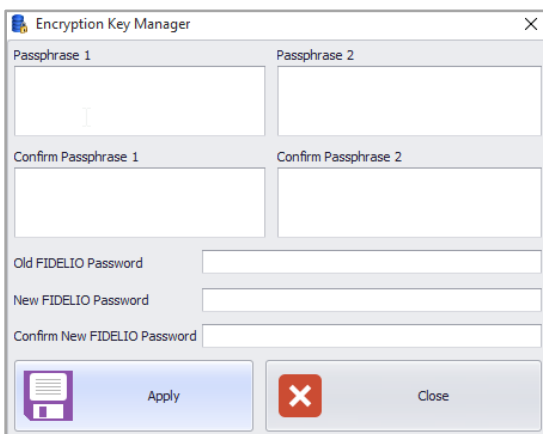


6. At the first launch of the program and if the database is yet to be upgraded, the only button available at the ribbon bar is **Upgrade DB to 8.0**. Click the button to upgrade the database.



**Figure 4 - OHC Tools Main Screen before DB Upgrade**

7. In the Encryption Key Manager window, enter the **Passphrase1** and **Passphrase 2, Old Fidelio password, Fidelio Password** and **Confirm** password. Ensure passwords entered are in the correct case as the **Old FIDELIO Password** is case-sensitive.



**Figure 5 - Encryption Passphrase**



- 
8. Click **Apply** to proceed. The system prompts *'The new passphrase has been changed...'* when the encryption completes. The Passphrase expiration is stored in "C:\Users\Public Document\Oracle Hospitality Cruise\OHCSecurity.par"  
Once the program is upgraded to 8.0, all programs other than the Launch Panel and Updater will be removed from the XAPP table.
  9. Copy the latest version 8.0.xx **Database Installer.exe** to "C:\Program Files (x86)\Oracle Hospitality Cruise" folder.
  10. Double-click the **Database Installer.exe** to execute the upgrade and follow the instructions of the upgrade wizard.
  11. When the application upgrade completes, navigate to "C:\Program Files (x86)\Oracle Hospitality Cruise" folder and launch the **Launch Panel** and then login using a 'Bypass Updater' by holding **ALT Key + click** on the female icon
  12. In the Launch Panel program, manually add these SPMS applications and DLL's to the respective group by pressing **F12** and select the group from the drop-down list.
    - a. Utilities group
      - i. Updater Watchdog.exe
    - b. System Files
      - i. OHCSPMSUI.dll
      - ii. OHCWebSockets.dll
    - c. REGASM Files
      - o CRUFLFC.dll
      - o OHCSPMSData.dll
      - o OHCSPMSBusiness.dll
      - o OHCSPMSMobile.dll
      - o OHCSPMSUtils.dll
  13. At the **Launch Panel, Utilities tab**, update the **Launch Panel, Updater** and **UpdaterAgent** program to the latest executable from the patch set downloaded, by right-clicking the program and select **Properties**, then click **Update file** and **OK** to save.
  14. Manually re-enter the modules to the **Property Management** tab and grant access to all User groups.
  15. Exit the Launch Panel program.
  16. Re-login to **Launch Panel without Bypass Updater** to update all the programs.  
A program **UpdaterWatchdog** is added to monitor and ensure the **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 Updater, restart the PC or switch user to Administrator, and manually restart **Updater** in Task Scheduler.
  17. 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.

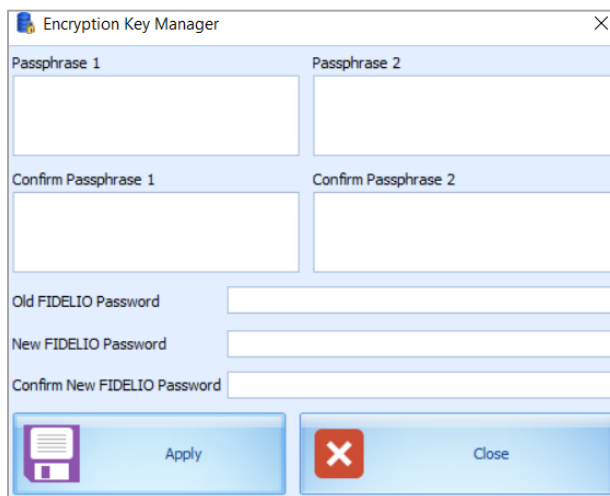
- 
18. Verify the following passwords are saved in `OHCSecurity.par`. Otherwise, manually update the password using **OHC Tools, Change Password** function.
    - VOIP Password
    - SMTP Password
    - MICROS Password
    - Credit Card merchant password

## Changing Database Encryption Key

The Change Database Encryption Key allows you 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.

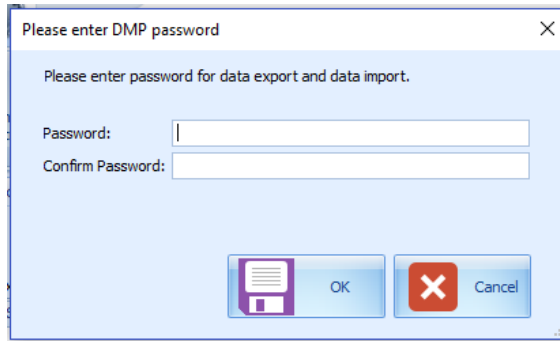
### Creating an Encryption Passphrase

1. Login to Tools application 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.



**Figure 6 - Encryption Passphrase**

3. Click **Apply** to proceed. The system prompts *'Please ensure there is no application is currently running in order to prevent data corruption later'*.
4. If Transparent Data Encryption (TDE) is used, the system performs a database backup that allows you to restore at a later stage. You are required to enter a password for the .DMP file and if an error occurs during the backup, will be prompt for the same password to be entered and they must be identical.



**Figure 7 - DMP Password Form**

5. Click **OK** to continue and program prompts a request to stop the running application, if any.
6. When the change encryption key begins, program performs a backup process on tables that need to be re-encrypted.
7. If data is found to be corrupted during encryption process, the system continues the process and prompts a warning at the end of the process before generating an error log.



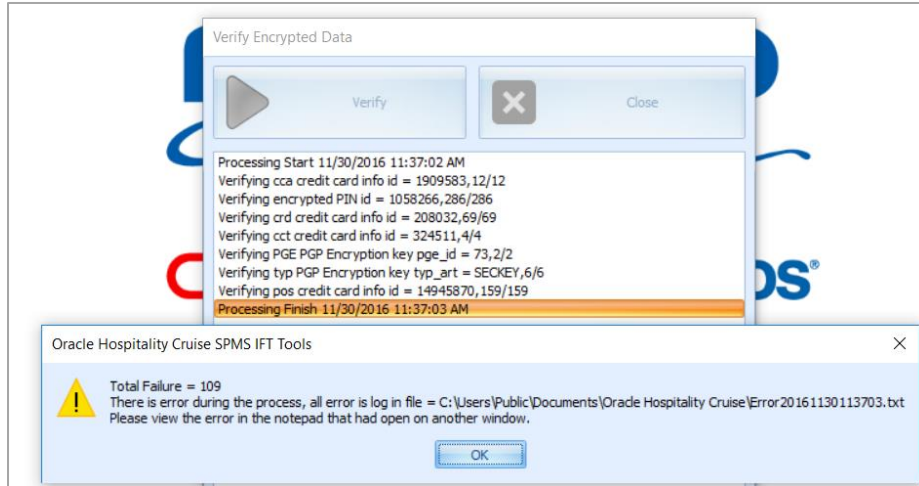
8. At the error prompt, choose **Yes** to continue replacing the encryption key or **No** to roll back the process by restoring the backup.
9. The Passphrase is saved in OHCSecurity.par and is valid for one year from the date of encryption.

## Verifying The Encrypted Database Data

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

### Verifying Encrypted Data

1. At the Tools application, select **Verify Database Encrypted Data** from the ribbon bar.
2. At the Verify Encrypted Data window, click **Verify**.
3. The Verify Database Encryption Data verifies data in User login credentials, Parameter, Reservation, POS Information, (PGP Key), Credit Card Registration, Transfer and Authorization
4. If the verification returns a failed message, possibility due to invalid data, correct the error and repeat the process.



**Figure 8 - Verify Database Encrypted Data**

5. Click **Close** when the process finishes.

## Changing 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.

You are not allowed to change the Ship's DB password when QCI Sync application is running and must have Database privilege granted before you are allowed to proceed.

1. In Tools window, select **Change Password** from the ribbon bar.
2. In Password Manger window, enter the system **User**, **System Password**, **Database User** and **Database Password** and password must fulfil the password specification.



**Figure 9 - Change Password Window**

3. Click **Apply** to update the database password and save the encrypted password to OHCSecurity.par.
4. Repeat the above steps to change the password for MICROS, SMTP and VOIP.

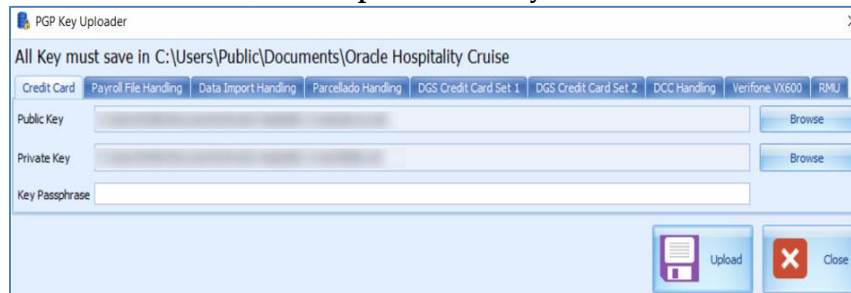
---

## Uploading PGP Key

The Upload PGP Key function is used to upload the Public Key (.pkr) and Private Key (.skr), a key pair for functionality that requires a Pretty Good Privacy (PGP) Key. For example, Payroll, Credit Card, DGS Resonline and Data Import handling. A key pair can only be generated using a third-party tool such as PortablePGP and FileAssurity OpenPGP. Refer to *PA-DSS 3.2 Implementation Guide* for more information.

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

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



**Figure 10 - PGP Key Uploader**

2. In the PGP Key Uploader window Credit Card tab, click the **Browse** button next to Public Key and select a .pkr file to upload. To upload a Private Key, click the **Browse** button next to Private Key to select a .skr file.
3. Enter the **Key Passphrase** if the key is generated with specific passphrase.
4. Click **Upload** to upload the keys. The system prompts 'Key upload is done successfully' when upload completes and stores both the encrypted keys in PGP table.
5. For DGS Credit Card handling, a key version is required.



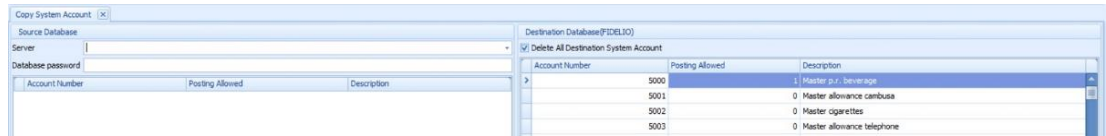
### NOTE:

The PGP Key has an expiry date and you must generate a new PGP Key and re-upload to the database once a reminder is prompt. Program does not allow you to reuse the same PGP Key

## Copying System Account

The Copy System Account function copies the System Account from one database to another database.

1. In the Tools window, select **Copy System Account** from the ribbon bar.
2. In Copy System account window, select the source database from the Server drop-down list and then enter the **User password**.
3. At the end of the ribbon bar, click **Connect** under the **Copy System Account** group. System Accounts shall populate on the left panel if the connection is successful.



**Figure 11 - Copy System Account**

4. Check the **Delete All Destination System Account** to add or remove the account in destination database. This is only possible when no posting exists in the account during copy process.
5. Click **Copy** to complete the process.

## Changing Log Trigger

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

1. In the Tools window, select **Change Log Trigger** from the ribbon bar.
2. In Create Change Log Trigger window, check the table on the left pane and then navigate to **Monitor Column** on the right pane.
3. In the **Monitor Column**, check the desire field for changes to be log into Payroll Audit Trail table and then navigate to Acc ID column tab.
4. In **Acc ID Column** tab, check the field to write into Payroll Contract Account ID.
5. Click **Create Change Log Trigger** at the ribbon bar to create the trigger.
6. Repeat the above steps to add more table field.

## Deleting 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 Audit Trail Deletion table.

1. In the Tools window, select **Delete Log Trigger** from the ribbon bar.
2. In the Create Deletion Log Trigger window, check the table on left pane and then navigate to **Description Column** on the right pane.
3. In the **Description Column**, check the field for changes to be to log into the Audit Trail table and then navigate to **Acc ID** column tab.
4. In **Acc ID Column** tab, check the field to write into Audit Trail Deletion Account ID.
5. Click **Create Deletion Log Trigger** at the ribbon bar to create the trigger.
6. System prompts a total of number of triggers deleted and created/upload. Click **OK** to continue
7. Repeat the above steps to add more table field.

## Inserting Log Trigger

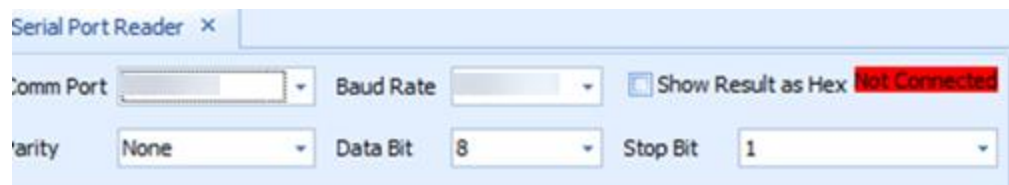
This function creates a trigger to log data insertion activities of the selected field. Any value deleted from these fields will log into Audit Trail Insertion table.

1. In the Tools window, select **Insertion Log Trigger** from the ribbon bar.
2. In Create Insertion Log Trigger window, select the table on left pane by checking the check box and then navigate to **Description Column** on the right pane.
3. In the **Description Column**, check the field for changes to be log into Audit Trail Insertion table and navigate to **Acc ID Column** tab and check the field value to write into Audit Trail Insertion Account ID.
4. Click **Create Insertion Log Trigger** at the ribbon bar.
5. The system prompts a total of number of triggers deleted and created/upload. Click **OK** to continue.
6. Repeat the above steps to add more table field.

## Serial Port Reader

The Serial Port Reader is a tool to test the reader connection with the barcode or card reader COM port.

1. Connect the device to the PC and click **Serial Port Reader** at the ribbon bar.
2. In Serial Port reader window, select the **Com Port, Parity, Baud Rate, Data Bit, Stop Bit**.
3. Check **Show Result** as 'Hex' to show the read result in Hexadecimal format.



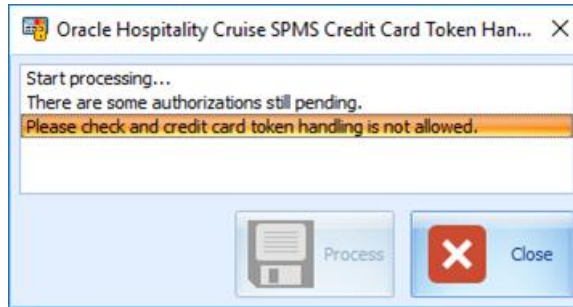
4. Click **Connect**. The connection indicator turns to green if the device is successfully connected.
5. Press the any button on the device to start reading a barcode. The result is shown in the text field.
6. Click **Clear All Text** to clear the field.

## Credit Card Token Handling

This function fixes the credit card data before transferring credit card data from non-token to token handling. This tool is a special tool use to ensure all existing Credit Card Authorization (CCA) and Credit Card Settlement (CCT) records are processed before changing the credit card format to SERVEBASE tokenization handling.

1. In the Tools window, select **Credit Card Token Handling** from the ribbon bar.
2. At the Credit Card Token Handling prompt 'By doing this, you are agreeing to use credit card tokenization handling', select **Yes** to agree or **No** to return to the main menu.

- At the Credit Card Token Handling prompt 'By doing this, you are agreeing to use credit card tokenization handling', select **Yes** to agree or **No** to return to the main menu.



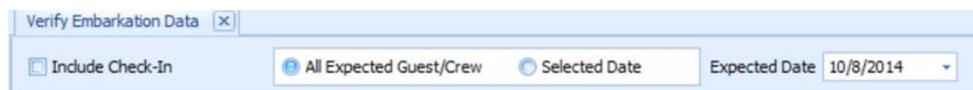
**Figure 12 - OHC Credit Card Token Handling**

- In Oracle Hospitality Cruise SPMS Credit Card Tokenization window, click **Process** and select **Yes** to implement the credit card handling.
- When **Yes** is clicked, verification of credit card will commence based on following criteria:
  - Parameter 'Not Specified', 'CC Transfer Format' is not 'SERVEBASE'.
  - No outstanding status for CCA record, where status is = 0)
  - No outstanding status for CCT record, where status is =0)
- If the above criteria are not met, the change token handling will not proceed and following message is shown in the dialogue box '*There are some authorizations still pending.*'
- Check and correct the CCA and CCT record and the repeat the above steps when ready.
- When the **Process** completes successfully, the system prompts a message '*Credit card token handling is implemented*'. The parameter 'Not Specified', 'CC Transfer Format' is updated to SERVEBASE and all credit card records are Deactivated.  
Manual activation is not allowed and the system prompts '*Settlement or reversal had done for this card, please get credit card again*'.

## Verifying Embarkation Data

This function validates and lists all VARCHAR2, CHAR fields that has ASCII value that are more than 127. For example: €, †, Œ, Ž, ‡, ©, ®. The verification validates the reservation fields used in Advanced Quick Check In application such as CAB, RES, CRD, SEC, SIG, USR, UXP, VIS\_BLOB, VIS\_TEXT.

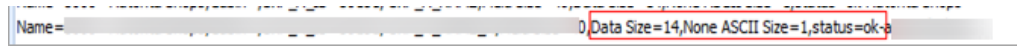
- In the Tools window, select **Verify Embarkation Data** from the ribbon bar.
- In Verify Embarkation Data window, select the guest reservation type by checking the **All Expected Guest / Crew** radio button or select a specified expected date and check if to **Include Check In**.





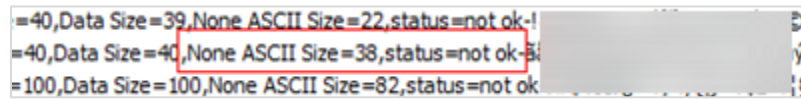
- Click **Verify Data** to proceed with verification. Below is the sample results shown in the verification window.

- The Non-ASCII code size less than 18 has status as *OK*.



**Figure 13 - Sample Non-ASCII Records Less Than 18 Characters**

- The Non-ASCII code size that are more than 18 will have status shown as *Not OK* and are prompt with '*There is potential x problem(s) found, please review the log file VERIFYDATA\_yyymmdd.txt*'.



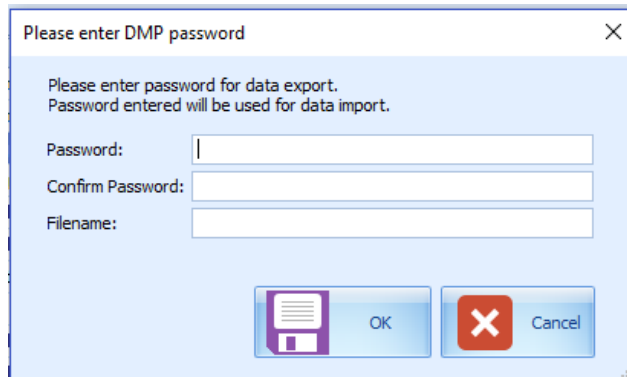
**Figure 14 - Sample Non-ASCII Code Value More Than 18 Characters**

## Exporting Database

The Export Database function enables you to export some of the data table from the database. The export process only exports table, data, index and trigger and does not export the view or sequence.

- In the Tools Import/Export tab, select **Export Database** from the ribbon bar.
- In the Export Database window, enter the 16 digits **Encryption Key** for the dump file.
- Select the table to export individually or click **Select All** at the ribbon bar for all tables.
- Click **Backup** at the ribbon bar to compress and encrypt the data table. The system prompts 'File had been backup to 'C:\<FilePath>\<Filename>' when the export is ready.

If TDE applies, the backup file will be stored as DATA\_PUMP\_DIR in the Oracle Database directory instead. You will be prompt to enter the DMP file password and filename.

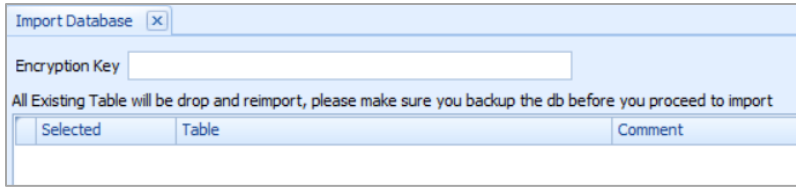


**Figure 15 - DMP Password**

- Click **OK** to close the window.

# Importing Database

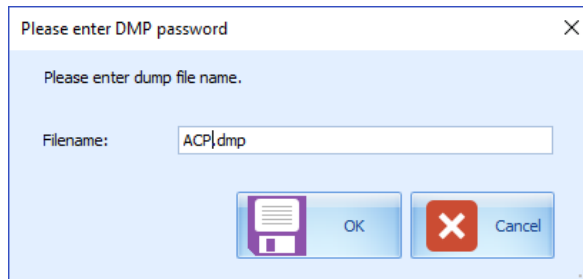
The Import Database function only imports data table of dump file exported using the above function.



**Figure 16 - Import Database**

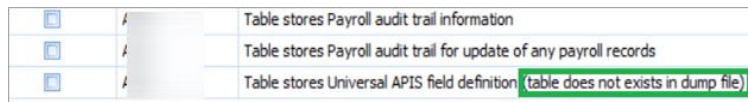
1. In Tools Import/Export tab, select **Import Database** from the ribbon bar.
2. In the Import Database window, enter **Encryption Key** of the dump file. The encryption key must match the key entered during database export in Tools application, Export Database function.
3. Click the **Select Dump File** at the ribbon bar and locate the file to import folder. If the Encryption Key does not match, you are prompted with message, 'Padding is invalid and cannot be removed. This could mean the encryption key is wrong.'

If TDE applies, you will be prompt to enter the DMP file name and password specified in step 4 of Export Database. In the event where the destination database is on another server, you are required to manually copy the DMP file from the source database server to the destination server, and then proceed to step 5.



**Figure 17 - DMP File Password**

4. List of tables populates on screen once the dump decompresses and decrypt successfully. This does not apply if TDE is used. Select the table to import.



**Figure 18 - Import Database - Table Excluded/Does Not Exist**

Table that does not exists in dump file are remarked with comment 'table does not exist in dump file' in the comment column. The system will drop and reimport all existing table during this process.

5. Click **Import Database** at the ribbon bar. The system prompt you to close all application before continuing.
6. Click **Yes** to stop the running instance and proceed with import. During import routine, the System drops the database tables and reimport all existing tables.

7. Once import completes, system prompts 'Import Database Completed, the log file will be show.'
8. Close the prompt to exit the application.

## Exporting Safety Setup

This function exports all the Safety setup from one ship to another. We recommend that you to use this tool with the new Muster List, In Port Manning and Safety Drill setup.

1. In the Tools Import/Export tab, select **Export Safety Setup** from the ribbon bar.
2. In Export Safety Setup window, check the desire the Safety setup and then click **Export** to export. Files are exported to C:\Users\Public\Documents\Oracle Hospitality Cruise\SafetySetup\_v8.xxx\_yyyymmdd.xml.'

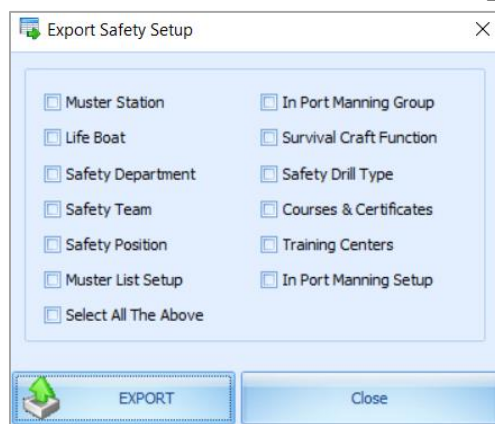


Figure 19 - Export Safety Setup

## Importing Safety Setup

This function is similar to Import Database function except that it only imports Safety Setup that were exported from Export Safety Setup in Tools application.

1. In the Tools Import/Export tab, select **Import Safety Setup** from the ribbon bar.
2. In Import Safety Setup window, click **SELECT FILE** to browse the XML file from Public Document folder.

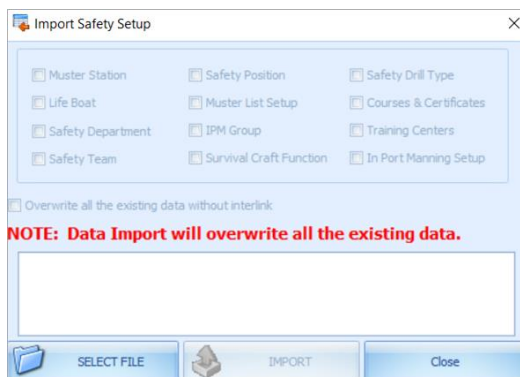
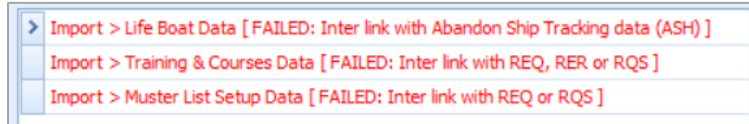


Figure 20 - Import Safety Setup

3. Check **Overwrite all the existing data without interlink** if you wish to overwrite existing data without interlink. The system does not overwrite data that has interlink to other tables and prompt the following message if interlink data are found 'System notified that there are some inter link table. System not going to overwrite existing data. Import Failed.'



**Figure 21 - Failed Import Safety Setup Message**

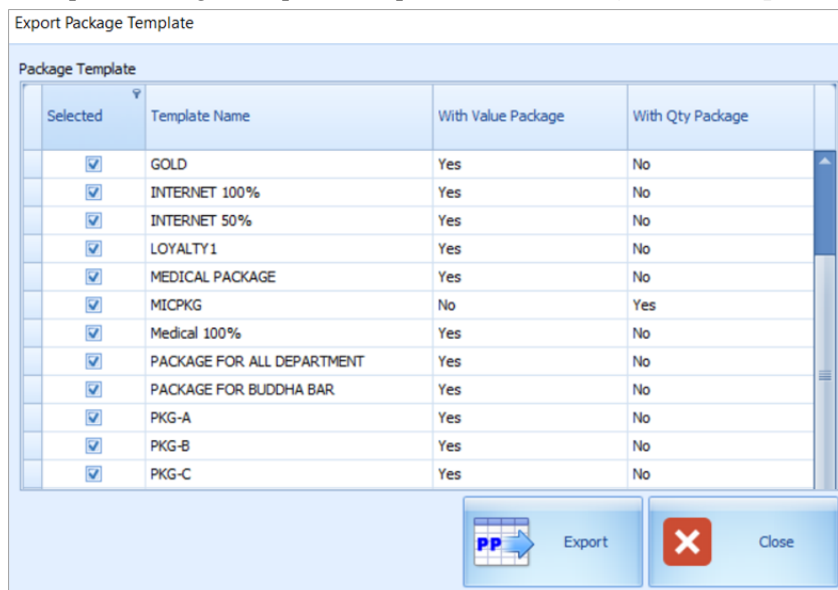
Completed course and certificate (COU) are not imported into database if record is found in require course and certificate (REQ), require substitution courses (RQS) and require course and certificate for each operation position (RER). The same applies to Muster List setup.

4. Click **Import** and select **Yes** when prompt 'There are existing data in either of this table (xxx,xxx). Are you sure want to overwrite?'
5. At the message prompt 'Import of Safety Setup Completed.', click **Close** to exit.

## Exporting Package Template

This function is used to duplicate the package plan template from one ship to another.

1. In Tools Import/Export tab, select **Export Package Template** from the ribbon bar.
2. In Export Package Template setup, select the **Package Plan Template** to export.



**Figure 22 - Export Package Template**

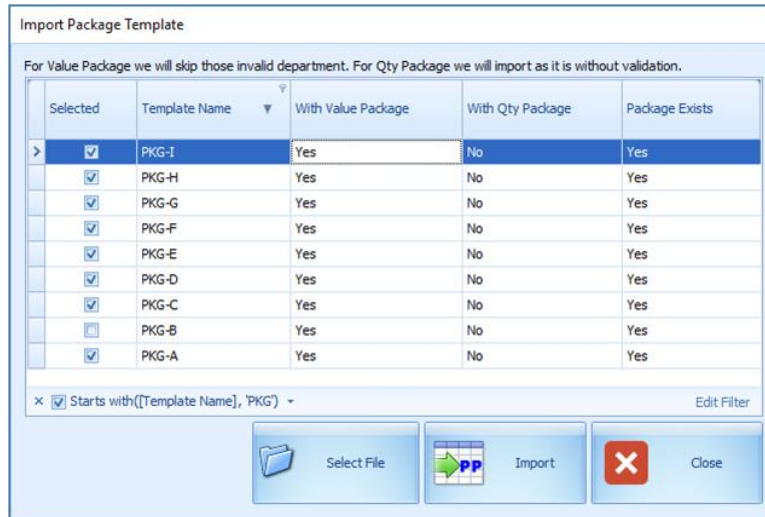
3. Click **Export** and browse the location to save the XML file.
4. Click **OK** when message prompt 'Export of Package Template Completed.'

---

## Importing Package Template

This function is used to import the package plan template exported from Export Package Template function in Tools application.

1. In the Tools Import/Export tab, select **Import Package Template** from the ribbon bar.
2. In Import Package Template window, click **Select File** to browse the XML file.



**Figure 23 - Import Package Template**

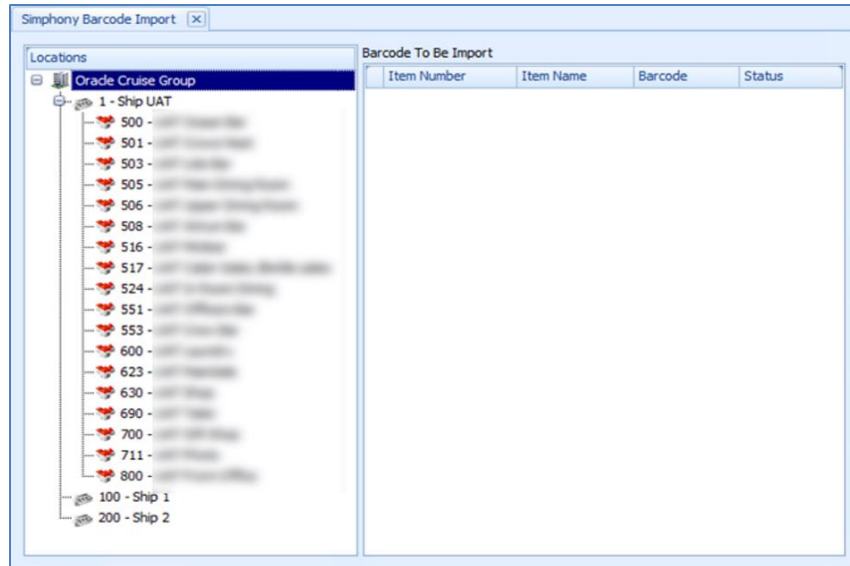
1. Check the template you wish to import from the **Selected** column.
2. Click **Import** to begin import.
3. At the message prompt 'Some of the template already exists in the DB, do you want to overwrite it?', click **Yes** to continue, and then **OK** to close the screen.

## Importing Barcode for Symphony

This function imports menu item barcode into Symphony database and requires a connection to Symphony System, setup in **Administration, System Setup, Parameter 'PROMO', 'Micros Server Name = 'hostname of Symphony database / Symphony',** and a username. The database password is entered using Change Password function in MICROS Password in Tools application.

When importing the barcode and the system prompts a message 'The Micros DB is not Symphony or the DB is offline.', this is due to the parameter 'Symphony', 'Micros Symphony Property Number' to copy the DB is invalid.

1. In the Tools Import/Export tab, select **Import Barcode for Symphony** from the ribbon bar and select the revenue center under the Locations section.



**Figure 24 - Symphony Barcode Import**

2. Click the **Load from CSV file**. Sample of the CSV file format are:
  - Field 1 = menu item object number
  - Field 2 = menu item name (for reference only)
  - Field 3 = barcode
3. You can then select to import from **Parent, Property ID** or in **Revenue Center**.  
When importing from Parent group, the Child group will follow. However, changes made to the Child group does not affect the Parent record. All new records will not have any status shown in the status column.
4. Click **Import** to proceed and the system prompt a message 'x record(s) imported, x record (s) failed to imported' when import completes. The program only imports valid item and non-duplicate item.