Oracle® Hospitality Cruise Shipboard Property Management System OHC Tools User Guide



Release 20.1 F33513-01 September 2020

ORACLE

Oracle Hospitality Cruise Shipboard Property Management System OHC Tools User Guide, Release 20.1

F33513-01

Copyright © 1995, 2021, Oracle and/or its affiliates.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Preface

1 OHC Tools Functionality

Verify Encrypted Database Data	1-2
Change Password	1-3
Upload PGP Key	1-4
Copy System Account	1-5
Change Log Trigger	1-6
Serial Port Reader	1-7
Credit Card Token Handling	1-7
Verify Embarkation Data	1-8
Export Database	1-8
Import Database	1-9
Export Safety Setup	1-10
Import Safety Setup	1-10
Export Package Template	1-11
Import Package Template	1-12
Import Barcode for Simphony	1-12



Preface

The OHC 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 project managers, application specialists and 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
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/.

Revision History

Table 1 Revision History

Date	Description of Change
September 2020	Initial Publication



1 OHC Tools Functionality

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

Figure 1-1 Functions in OHC Tools Home Tab



Figure 1-2 Functions in OHC Tools Import/Export Tab

	🔒 🛈 E	3		Oracle I	Hospitality Cruis	se SPMS OHC To	ols	· _
Home Impo	Impo	ort/Ex	port					
stm								
		- Lee	L	₽ ₽	PP 🔶			
1	Import	Import	Export	Import Package	Export Package	Import Barcode		
Di	atabase	Safety Setup	Safety Setup	Template	Template	for Simphony		
			Import/	Export				

Change 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 Password, New Password, and Confirm New Password.
- 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, allowing you to restore at a later stage. This requires a password for the DMP file. If an error were to occur during the backup, you will be prompt to enter the same password and they must be identical.



Please enter DMP pa	ssword	×
Please enter passw	ord for data export and data import.	
Password:		
Confirm Password:		
	OK Cancel	

- 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 corrupted data is found during the encryption process, the system continues the process and prompts a warning at the end of the process before generating an error log.

Fi	gur	e 1-4	Encryption Failed Warning
		Please v	error during the process, all error is log in file = iew the error in the notepad that had open on another window. want to continue? (Yes - Ignore Error and Continue, No = Abort and Restore from Backup)
			Yes No

- 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.

Verify 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.

- 1. At the Tools application, select **Verify Database Encrypted Data** from the ribbon bar.
- 2. At the Verify Encrypted Data window, click Verify.
- 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 1-5 Verify Encrypted Database

Verify Encrypted Data	
Verify	Close
Processing Start 11/30/2016 11:37:02 AM Verifying cca credit card info id = Verifying typ PGP Encryption key typ_art = Verifying pos credit card info id = 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 Please view the error in the notepad that had open on another window.	

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

Change Password

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

You are not allow 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.



Figure 1-6	Password	Manager	Window
------------	----------	---------	--------

🔒 Password Manage	er			×
Database Password	Micros Password	SMTP Password	Voip Password	·
Service Name				
System User				
System Password				
Database User				*
Database Password				
		Apply		Close

- 1. In Tools window, select Change Password from the ribbon bar.
- In Password Manger window, enter the system User, System Password, Database User, and Database Password and password must fulfil the password specification.
- **3.** Click **Apply** to update the database password and save the encrypted password to OHCSecurity.par.
- 4. Repeat the steps above to change the password for MICROS, SMTP and VOIP.

Upload PGP Key

The Upload PGP Key function is used to upload the Public Key (.pkr) and Private Key (.skr), a key pair for function that requires a Pretty Good Privacy (PGP) Key. For example, Payroll, Credit Card, DGS Resonline and Data Import handling. You can only generate a key pair using a third party tools such as PortablePGP and FileAssurity OpenPGP. See *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.



Figure 1-7 PGP Key Uploader

FOR Rey Of	ploader						
All Key mu	st save in C:\Us	sers\Public\Docur	nents\Oracle Ho	spitality Cruise			
Credit Card	Payroll File Handling	Data Import Handling	Parcellado Handling	DGS Credit Card Set 1	DGS Credit Card Set 2	DCC Handling	Verifone VX600 RMU
Public Key							Browse
Private Key							Browse
Key Passphrase	e						

- 1. In the Tools window, select Upload PGP Key from the ribbon bar
- 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 generate with specific passphrase.
- Click Upload to upload the keys. The system prompts 'Key upload is done successfully' when upload completes and stores both the encrypted keys in TYP_PGP table.
- 5. For DGS Credit Card handling, a key version is required.

Note:

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

Copy 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. The System Accounts shall populate if the connection is successful.

Figure 1-8 Copy System Account

Source Database				D	estination Database				
Server			*	¥.	Delete All Destination System Accourt	t			
Database password					Account Number	Posting Allowed		Description	
Account Number	Posting Allowed	Description	1	>	50	00	1	Master p.r. beverage	
					50	01	0	Master allowance cambusa	
					50	02	0	Master cigarettes	
					50	03	0	Master allowance telephone	



- 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.

Change Log Trigger

The following function creates a Database Trigger that logs changes made to selected fields. Values from the selected fields are stored 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 required change fields to 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.

Delete Log Trigger

This function creates a Database Trigger that logs data deletion activities of the selected fields. Values deleted from the selected fields will be logged into Audit Trail Deletion table.

- 1. In OHC Tools, select **Delete Log Trigger** from the ribbon bar.
- 2. From the Create Deletion Log Trigger window, navigate to the **Description** column
- 3. Listed under the Description column, select all the fields so that their changes will be logged into the SDR table
- 4. Navigate to the Acc ID column tab.
- 5. In Acc ID Column tab, select the fields that will be written into the SDR_ACC_ID
- 6. Click **Create Deletion Log Trigger** on the ribbon bar to create the database trigger.
- 7. The system will prompt a total of number of database triggers that tracks fields deleted and also track fields created/upload. Click **OK** button to continue.
- 8. Repeat the steps above to add more table fields.

Insert Log Trigger

This function creates a Database Trigger that logs data insertion activities of the selected fields. Values added from the selected fields will be logged 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**, select the fields log into the Audit Trail Insertion table.



- 4. Navigate to Acc ID Column tab, and select the field to write into Audit Trail Insertion Account ID.
- 5. Click Create Insertion Log Trigger at the ribbon bar.
- The system will prompt a total of number of database triggers that tracks fields deleted and also track fields created/upload. Click OK to continue.
- 7. 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.

Figure 1-9 Serial Port Reader Setting

Serial Port	Reader ×							
Comm Port	СОМЗ	•	Baud Rate	9600	+	Show F	Result as Hex	Not Connected
arity	None	-	Data Bit	8	*	Stop Bit	1	+

- 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 the **Show Result as Hex** checkbox to show the read result in Hexadecimal format.
- 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 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 from a non-token authorization to token handling. This special tool is used to ensure all existing Credit Card Authorization (CCA) and Credit Card Settlement (CCT) records are process before changing the credit card format to SERVEBASE Tokenization handling.

- 1. In the Tools window, select Credit Card Token Handling from the ribbon bar.
- 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.
- In Oracle Hospitality Cruise SPMS Credit Card Tokenization window, click the Process and select Yes to implement the credit card handling.

ORACLE

- 4. When **Yes** is clicked, verification of credit card will commence based on following criteria:
 - a. Parameter 'Not Specified', 'CC Transfer Format' is not 'SERVEBASE'.
 - **b.** No outstanding status for CCA record, where status is = 0
 - c. No outstanding status for CCT record, where status is =0
- 5. If the above criteria are not met, the change token handling will not proceed and following message will show 'There are some authorizations still pending'.
- 6. Check and correct the CCA and CCT record and the repeat the above steps when ready.
- 7. 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'.

Verify Embarkation Data

This function validates and lists all VARCHAR2, CHAR fields that has ASCII value of 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.

- 1. In the Tools window, select Verify Embarkation Data from the ribbon bar.
- 2. In Verify Embarkation Data window, check the relevant options and **Include Check In** if you want to include check ins.
- 3. 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 characters will have status as OK.
 - The Non-ASCII code size that are more than 18 will have status shown as *Not OK* and listed with '*There is potential x problem*(s) *found, please review the log file VERIFYDATA_yyymmdd.txt*'.

Figure 1-10 Verify Embarkation Data

0 Data Size=14,None ASCII Size=1,status=ok-a		
=40,Data Size=39,None ASCII Size=22,status=not ok-!	1980	
=40,Data Size=40,None ASCII Size=38,status=not ok-		
= 100,Data Size = 100,None ASCII Size = 82,status = not ok	 	10

Export Database

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



- 1. In the Tools Import/Export tab, select Export Database from the ribbon bar.
- 2. In the Export Database window, enter the 16 digits **Encryption Key** for the dump file.
- 3. Select the table to export individually or click **Select All** at the ribbon bar for all tables.
- 4. 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 Password** and **Filename**.

5. Click **OK** to confirm and close the window.

Import Database

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

Figure 1-11 Import Database

Import Databas	e 🗙		
Encryption Key	will be dree and reimport	please make sure you backup the db b	afore you proceed to import
Selected	Table	Jease make sure you backup the up b	Comment

- 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 browse the file to import.
- 4. If the Encryption Key does not match, you are prompt 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 mentioned in step 4 of Export Database. If the destination database is on another server, copy the DMP file from the source database server to the destination server first before proceeding to step 5.

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

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



- 6. Click **Import Database** at the ribbon bar. You will be prompt to close all application before continuing.
- 7. Click **Yes** to stop the running instance and proceed with import. During the import routine, the system drops the database tables and re-import all existing tables.
- 8. Once import completes, system prompts '*Import Database Completed, the log file will be show.*'
- 9. Close the prompt to exit the application.

Export 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.

	Export Safety Setup		\times
	Muster Station	🔲 In Port Manning Group	
	🔲 Life Boat	Survival Craft Function	
	Safety Department	Safety Drill Type	
	Safety Team	Courses & Certificates	
	Safety Position	Training Centers	
	Muster List Setup	In Port Manning Setup	
	Select All The Above		
1	EXPORT	Close	

Figure 1-12 Export Safety 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_yyymmdd.xml.'

Import Safety Setup

This function is similar to the Import Database function with the exception that it *only* import Safety Setup that are export from Export Safety Setup in Tools application.

1. At the Tools Import/Export tab, select Import Safety Setup from the ribbon bar.



2. At the Import Safety Setup window, click **SELECT FILE** to browse the XML file from Public Document folder.

Figure 1-13 Import Safety Setup

Muster Station	Safety Position	🔲 Safety Drill Type
🔲 Life Boat	Muster List Setup	Courses & Certificates
🔲 Safety Department	IPM Group	Training Centers
🔲 Safety Team	Survival Craft Function	🔝 In Port Manning Setup
remained on one enoungs	lata without interlink	

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 an inter link to other tables and prompt the following message if inter link data is found 'System notified that there are some inter link table. System not going to overwrite existing data. Import Failed.'

Completed course and certificate (COU) are not import into database if the 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.

Export Package Template

This function duplicates the package plan template from one ship to another.

- 1. At the Tools Import/Export tab, select **Export Package Template** from the ribbon bar.
- 2. At the Export Package Template setup, select the **Package Plan Template** to export.
- 3. Click **Export** and browse the location to save the XML file.
- 4. Click OK when message prompt 'Export of Package Template Completed.'



Import Package Template

This function imports the package plan template exported from Export Package Template function in Tools application.

- 1. At the Tools Import/Export tab, select **Import Package Template** from the ribbon bar.
- 2. At Import Package Template window, click Select File to browse the XML file.
- 3. Check mark the template you wish to import from the **Selected** column.
- 4. Click Import to be begin import.
- 5. 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 window.

Import Barcode for Simphony

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

When importing the barcode and the system prompt a message '*The Micros DB is not Simphony or the DB is offline.*'. This is due to the parameter '**Simphony', 'Micros Simphony Property Number'** that is use to copy the DB is invalid.

- 1. At the Tools Import/Export tab, select **Import Barcode for Simphony** from the ribbon bar and select the revenue center under the **Locations** section.
- 2. Click Load from CSV file. Sample in 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 select to import from Parent, Property ID or in Revenue Center.
- 4. 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.
- 5. Click **Import** to proceed and the system prompt a message '*x* record(s) imported, *x* record (s) failed to imported' when the import completes. The program only import valid item and non-duplicate item.

