

Oracle® Hospitality Cruise Fleet Management User Guide



Release 9.1
F13416-09
November 2022

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2004, 2022, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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®, Java, and MySQL 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 Fleet Management Components

2 Security Server

Security Server Encryption	2-1
Secure Clients	2-2
Configuring OHCFMSSecurity Service	2-3
Importing the Self-Signed Certificates	2-3
Adding HTTPS Binding	2-4
Updating the Configuration File	2-6
Frequently Asked Questions and Troubleshooting	2-6
Internet Information Services (IIS) Set Up	2-7
Setting Up IIS on Microsoft Windows 7	2-7
Setting Up IIS on Microsoft Windows Server 2008 and 2008 R2	2-7
Setting Up IIS on Microsoft Windows Server 2012	2-7
Setting Up IIS on Microsoft Windows Server 2016	2-8

3 About Oracle Hospitality Cruise Fleet Management Viewer

4 The FMS Login Screen

5 The FMS Dashboard

Overview of Guest Relation Management	5-2
Viewing Guest Details	5-2
Viewing Group Management	5-3
Viewing Shore Excursion Management	5-3
Customizing Statistical Analysis	5-3

Exporting a Template	5-4
Financial Classifications	5-5
Setting Classifications Types	5-6
Shore Side Departments	5-7
Hotel Operation	5-7
Customer Service Department	5-8
Onboard Revenue Department	5-8
Finance Department	5-9
Marketing Department	5-9
Adding and Editing a Ship	5-10
Change Logs and Error Logs Details	5-11
Adding Users and Groups	5-12
Logging And Security Shore-Side	5-12
Active Directory Integration In Fleet Management System	5-13

6 Universal Check In XML Generator

Messaging Process	6-1
Settings	6-1

7 Database Schema Password Manager

Migrating Schema Entries to the Latest Encryption	7-1
Changing Schema Passwords	7-2
Adding a Schema Entry	7-3

8 Database Updater

Database Updater Login Screen	8-1
-------------------------------	-----

9 Corporate Data Transfer Interface

Methods of Data Transfer	9-1
Message Formats	9-1
Types of Data Transfer	9-2
Type of Connections	9-2
Message Structure	9-2

10 Watchdog

Adding a New Rule	10-1
-------------------	------

11 Reservations Online

General Setup	11-2
Ships Decode	11-2
Data Processing	11-3
Source Data Filtering	11-4
Reservations Messaging Process	11-4
Interface - Import Reservations To The Ship Database	11-4
Reservation Status	11-5
Reservation Status Alerts	11-5

12 Sender and Receiver Data Transfer Interface

Configuring Sender	12-1
Setup and Configuration	12-4
Interface Preparation and Best Practices	12-7
Prerequisites	12-7
Receiver	12-7
Syncing Data	12-10
Tracking Record (Batch Level)	12-11
Record Level Tracking Process	12-11
Tracking Records Setting Steps	12-11

13 Corporate Access Module

Business Flow	13-2
Visitors	13-3
Approvals	13-4
My Request Form	13-5
Crew Family Details Form	13-5
Orphaned Emails Form	13-5
Crystal Reports	13-5
Setup	13-5
General	13-8

14 Report Auto Sequencer

15 Encryption Manager (EM)

Changing FMS Encryption Key	15-3
Before You Begin	15-3
Steps to Change the FMS Encryption Key	15-3

16 Emergency Response System (ERS)

Logging in to Emergency Response System	16-1
Activating Emergency Record Transfer	16-1
Viewing Vessels in Emergency	16-2
Viewing Passenger Details	16-2

17 Gangway Activity

Viewing Gangway Activity	17-1
--------------------------	------

Preface

Oracle Hospitality Cruise Fleet Management System (FMS) is a solution that provides the shore side users access to the ship data for compliance, analytic, and marketing purposes.

Audience

This document is intended for the users, technical personnel, support and consulting personnel who are seeking information regarding the Fleet Management.

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
- 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
August 2019	Initial Publication
September 2019	<ul style="list-style-type: none">• Removed the Itinerary Tracker chapter. Front end of the module is not included in this release.• Renamed the FMS Welcome Screen Application chapter.• Updated the Overview of Guest Relation Management section.
October 2019	Updated the Tracking Record Batch Level section.
November 2019	Updated the Watchdog section.
February 2021	Added content for FMS Key Rotation.
August 2021	Added content for Encryption Key tab and GCM Mode information.

Date	Description of Change
November 2021	Added Config-Settings table reference to Configuring Sender section. Revised Sender/Receiver section to include MOD Date Adjustment Hours
January 2022	Removed outdated topic Resonline for Adding and Editing Ship Added steps to change PGP Keys in FMS and SPMS
November 2022	Removed Workflow section from the guide Made minor grammatical correction Reorganized content flow

1

Fleet Management Components

Fleet Management (FM) is comprised of the following components.

- Oracle Hospitality Cruise Emergency Response System (ERS)
- Oracle Hospitality Cruise Gangway Activity
- Oracle Hospitality Cruise Encryption Manager (EM)
- Oracle Hospitality Cruise Security Server
- Oracle Hospitality Cruise Sender And Oracle Hospitality Cruise Receiver
- Oracle Hospitality Cruise Corporate Data Transfer Interface
- Oracle Hospitality Cruise Watchdog
- Oracle Hospitality Cruise Report Auto Sequencer

Fleet Management (FM) is comprised is of the following add-ons:

- Oracle Hospitality Cruise Corporate Access Module
- Oracle Hospitality Cruise ResOnline
- Oracle Hospitality Cruise Universal Check In XML Generator



Note:

In Fleet Management components, Database Password Manager and Encryption Manager are not part of the Fleet Management Suite. They are provided separately.

2

Security Server

FMS Security Server hosts sensitive information like FidelioBK schema password and KEK key. It stores these two parameters in encrypted form in the configuration file. It uses Data Protection Application Programming Interface (DPAPI), a Windows based encryption and machine level key for the encryption.

Security Server Encryption

Fleet Management Security Server hosts sensitive information in an encrypted form in the configuration file. You should run the server with Administrative privilege.

The below examples shows both the FidelioBK schema password and Key Encryption Key(KEK) key in plain text and encrypted format:

Schema password and KEK in plain text.

```
<?xml version=1.0 encoding=utf-8 ?>
<configuration>
  <appSettings>
<add key="FidelioBkPwd" value="" />
<add key="KEKKey" value="" />
<add key="ServiceUrl" value="https://localhost/OHCFMSSecurityService/
FCTransactionsService.asmx"/>
<add key="TNSNamesPath"
value="C:\Oracle\OraHome12c\network\admin\tnsnames.ora"/>
</appSettings>
```

Schema password and KEK in encrypted form:

```
<?xml version=1.0 encoding=utf-8 ?>
<configuration>
  <appSettings
configProtectionProvider=DataProtectionConfigurationProvider>
  <EncryptedData>
    <CipherData>
<CipherValue>AQAAANCMnd8BFdERjHoAwE/
Cl+sBAAAA0rBRLmkdWUumfaBJzssrgwQAAAAACAAAAAADZgAAwAAAAABAAAAAjrjz1Mv9n/
9YTWeJObreGAAAAAASAAACgAAAAEAAAAE7s1WJ6avIdjl/
xJCFSHxXAAQAADGvQLFOHv5bbu8yElnDggZyC4g441wOzgp0l5Z1SxmmlV0ZF1W+3jE1b0d7JQnGS
U5oiJ9IcXicYWUOhFPZuHSHLf3jVvazGOqFVYyUX/
PlsJ7KLAwbNIosYItbj8C5u+fCLasFWd7RTjkJUh/
ToqsUMHrPYwqzbeNe6tq9dngHoboA0DrI5tLjqBaQnaqxhMAYd3N1lBRPfnPDq2ah5nJoMT0jpsbz
GvfzQ9lxB1FaIk4ntdYcn3V9Lo2sn9zSHrFu/
DbdeHN+xHtehFuUC4wlzAc+h120y87tXuI72z5txCEsRwKM7tPqibqlvtje/
si8H0SSzu5oA8P2tN1rzun+bd5il//
vQG74WxgwWeMLA4gXbRg6Re7yXQDlmgNaqf36SEx7mtZa4TjjjYIkz2LkSxXDUuTiSYNd5w18N2xJ
yn8rXpV0zZeI8kKIAU/WP1aGWR5fvwtmfUskc+K3a7A23epLY8/
fG2IqaVdiIXq8ZpoLPoT+ksL4DTLz6TyIn54Mj7y0+kqaeR7fYxv1wCiZzNTcVtjtcnPneu4f7GOL
```

```
jsn6Ujyk08b0++YjpfzLRyYNjBuuXp4DPynPKSpAoqhQAAADhdk==  
</CipherValue>  
  </CipherData>  
</EncryptedData>  
</appSettings>
```

Secure Clients

On startup, any client (applications/interfaces/web services) connecting to the server for the first time will fetch and store the FidelioBK password and Encryption Key (KEK) in an encrypted form in their configuration files. Thereafter, the client will use the FidelioBK password and the KEK stored in the configuration files. The client will need to reconnect to the server if there is a change in the FidelioBK password or KEK key.

To update FidelioBK password and Key Encryption Key, open OHC Security Server, Administration and provide the relevant credentials

Figure 2-1 Server Logs for Successful Secure Client Connection

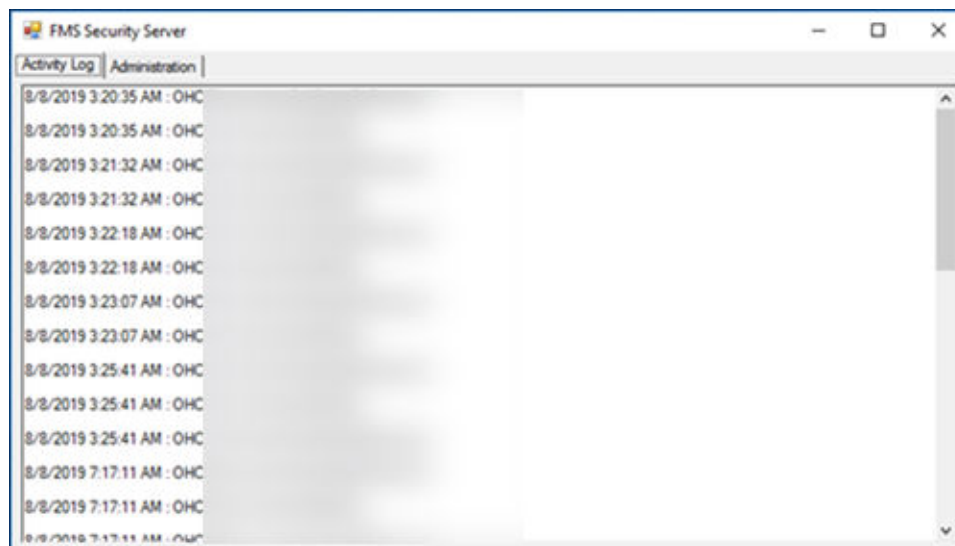
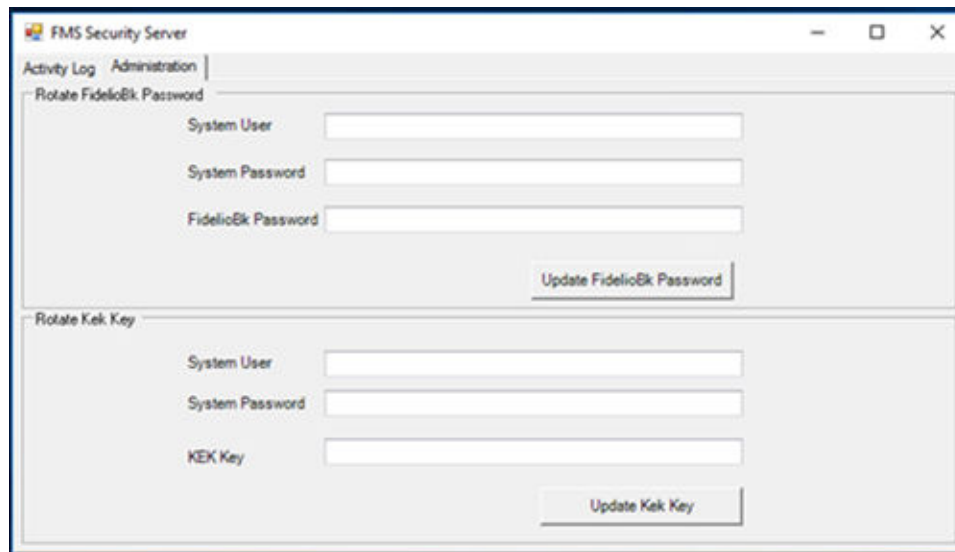


Figure 2-2 FidelioBK Password and KEK Key Fields on the Administration Tab



Configuring OHCFMSSecurity Service

1. Go to `C:\inetpub\wwwroot\OHCFMSSecurityService` and open `Web.Config` file
2. Update `TNSNamesPath` with the correct path for `tnsnames` file. Below is the example.

```
<appSettings>
<add key="FidelioBkPwd" value="" />
<add key="KEKKey" value="" />
<add key="ServiceUrl" value="https://localhost/OHCFMSSecurityService/
FCTransactionsService.asmx/>
<add key="TNSNamesPath"
value="C:\Oracle\OraHome12c\network\admin\tnsnames.ora"/>
</appSettings>
```

3. Update the data source name in the connection string.

```
<connectionStrings><add name="OracleDBServer" connectionString="Data
Source=OHCFMS;User ID={0};Password={1}"
providerName="System.Data.OracleClient"/>
</connectionStrings>
```

Importing the Self-Signed Certificates

Importing Self-signed certificates using the Microsoft Management Console (MMC).

1. To import the PFX into the local computer's Trusted Root Certification Authority Certificates folder.
 - a. Click the **Windows Start** button and select the **Run** command.
 - b. Enter **MMC** and click **OK**.
 - c. Select **File**, and click **Add / Remove Snap In**.

- d. Double-click **Certificates**.
 - e. Select the computer account, select **Local Computer**, and then click **Finish**.
 - f. Click **OK** to close the Snap-In window.
 - g. Click **[+]** to expand the **Certificates** container, then select **Trusted Root Certification Authorities**, and **Certificates**.
 - h. Right-click **Certificates**, select **All Tasks**, and click **Import**.
 - i. At the Certificate Import Wizard, click **Next**.
 - j. Click **Browse**, select the PFX to import, and then click **Open**.
 - k. Click **Next**.
 - l. Select **Place all certificates in the following store**. Ensure the **Trusted Root Certification Authorities** is visible in the **Certificate Store** section and click **Next**.
 - m. Click **Finish**, and then click **OK**.
2. To import the PFX file into the local computer's Personal Certificates folder.
 - a. Click the **Windows Start** button and select the **Run** command.
 - b. Enter the **MMC** and click **OK**.
 - c. Select **File**, and click **Add / Remove Snap In**.
 - d. Double-click **Certificates**.
 - e. Select the computer account, followed by **Local Computer**, then click **Finish**.
 - f. Click **OK** to close the Snap-In window.
 - g. Click **[+]** to expand **Certificates** container and select **Personal**, and **Certificates**.
 - h. Right-click **Certificates**, select **All Tasks**, and click **Import**.
 - i. At the Certificate Import Wizard, click **Next**.
 - j. Click **Browse**, select the PFX to import, and then click **Open**.
 - k. Click **Next**.
 - l. Select **Automatically select the certificate store based on the type of certificate**.
 - m. Click **Finish**, and then click **OK**.

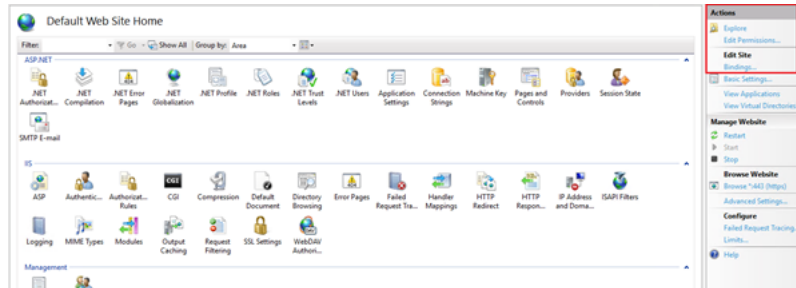
Adding HTTPS Binding

After setting up an Internet Information Services (IIS), the IIS will use the default port 80 and the binding is HTTP. To add HTTPS binding, create a certificate or buy a certificate from service providers.

1. In **Internet Information Services (IIS) Manager**, under **Connections**, expand your server's name, and then expand **Sites**. **OHCfMSsecurityService** can be seen under the default web sites.
2. Right-click **OHCfMSsecurityService**, and then click **Convert to Application**.
3. Select the **OHCfMSsecurityService** website for which you want to install the SSL Certificate.

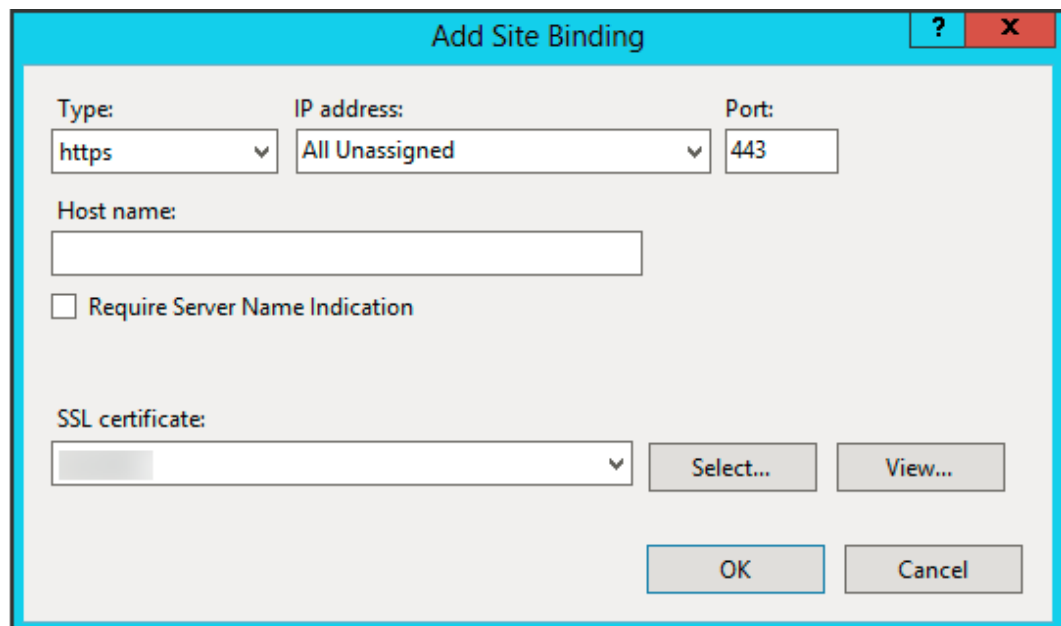
4. In the **Actions** menu, select the **Bindings** option under **Edit Site**.

Figure 2-3 HTTPS Binding option



5. In the Site Bindings window, click **Add**.
6. In the Add Site Binding window, enter the following information:
 - For **Type**, select **HTTPS** from the drop-down list.
 - For **IP Address**, select **All Unassigned** from the drop-down list.
 - For **Port**, enter 443. If you are using a non-standard port for SSL traffic, enter that port number.
 - For **SSL Certificate**, select the recently imported SSL Certificate from the drop-down list.

Figure 2-4 Add Site Binding



7. Click **OK**. The SSL Certificate is now installed.
8. To test the HTTPS binding:
 - a. Select **IIS Web Site**, and then select **Browse *:443(HTTPS)** from the right panel. The IIS home page opens in a web browser.

- b. If you use a self-signed certificate, the browser will show a certificate error. To proceed, accept the certificate exception and if you have a self-signed certificate, it will not show the certificate error and it displays the IIS home page with HTTPS instead.

Updating the Configuration File

To run the Security Server application, you must add or update the `<appSettings>` section in the Configuration file.

1. For Microsoft Windows applications, open the `app.config` file for editing.
For Web applications, open the `web.config` file for editing.
2. Ensure the `<appSettings>` section is added/updated as follows:

```
<appSettings>
  <add key="FidelioBkPwd" value="" />
  <add key="KEKKey" value="" />
  <add key="ServiceUrl" value="" value="https://localhost/
OHCFMSSecurityService/FCTransactionsService.asmx"/>
  <add key="TNSNamesPath"
value="C:\Oracle\OraHome12c\network\admin\tnsnames.ora" />
</appSettings>
```

Frequently Asked Questions and Troubleshooting

- Where is the Security Server installed?
The Security Server is installed on the IIS Machine.
- Who uses the Security Server?
 - An IT manager at the client site or
 - An administrator at the client site or
 - A support personnel
- What is the purpose of the Security Server?
The Security Server is used to host sensitive information like FidelioBK password and KEK key.
- What kind of logs are available for the Security Server?
 - An Activity Log capturing information of a client connection and is stored in the installation directory
(C:\inetpub\wwwroot\OHCFMSSecurityService\bin\Log).
 - An Exception Log stored in inetpub folder
(C:\inetpub\wwwroot\OHCFMSSecurityService\bin>Error).
 - A Trace Log that is used when the above logs information are insufficient for troubleshooting. Tracing can be enabled on the server and client configuration files using the `<system.diagnostics>` section that generates a detailed trace file called (`messages.svxlog`) which contain information of the errors messages and warnings. You can view the trace log file with `SvcTraceViewer.exe` tool. To avoid

creating a large trace log, the tracing needs to be disabled once you obtain the information for the troubleshooting.

Internet Information Services (IIS) Set Up

The following sections describe the steps to set up IIS based on your operating system (OS):

Setting Up IIS on Microsoft Windows 7

1. In **Start** menu, select **Control Panel**, and then click **Programs**.
2. Under **Programs and Features**, select **Turn Windows features on or off**.
3. In the **Windows Features** list, expand **Internet Information Services**, and then expand **World Wide Web Services**.
4. Expand **Common HTTP Features**, and then select **Static Content**.
5. Optional: To manage local and remote web servers and sites, install Internet Information Service (IIS) Manager by selecting **Internet Information Services**, expanding **Web Management Tools**, and then selecting **IIS Management Console**.
6. Click **OK** to complete the installation.
7. In the **Windows Features** list, expand **Microsoft .NET Framework**, and then select **Windows Communication Foundation HTTP Activation**.
8. To verify that the web server has been installed correctly, at the browser address bar, type `http://localhost`. The default web site opens and displays the IIS image. If the IIS image does not appear, then verify that you have configured static content on IIS, as described in step 4.

Setting Up IIS on Microsoft Windows Server 2008 and 2008 R2

1. In the **Start** menu, select **All Programs**, select **Administrative Tools**, and then click **Server Manager**.
2. In the navigation pane, select **Roles**, and then click **Add Roles**.
3. In the Before You Begin window, click **Next**.
4. In the Select Server Roles window, select **Web Server (IIS)**, click **Next**, and then click **Next** again.
5. In the Select Role Service window, expand **Common HTTP Features** and then select **Static Content**. Other features that are selected by default can remain selected.
6. Click **Next**, confirm your selections, and then click **Install** to complete the installation.
7. When the installation is complete, click the **Close** button.
8. To verify that the web server has been installed correctly, at the browser address bar, type `http://localhost`. The default website opens and displays the IIS image. If the image does not appear, then verify that you have configured static content on IIS, as described in step 5.

Setting Up IIS on Microsoft Windows Server 2012

1. In the Start page, select **Server Manager**.

2. In the navigation pane, select **Dashboard**, and then click **Add roles and features**.
3. In the Add Roles and Features wizard, on the Before You Begin screen, click **Next**.
4. In the Select Installation Type screen, select **Role-based** or **feature-based** installation, and then click **Next**.
5. In the Select Destination Server screen, click **Select a server from the server pool**, select your server from **Server Pool** list, and then click **Next**.
6. In the Select Server Roles screen, select **Web Server (IIS)**, and then click **Next**.
7. Click **Next**.
8. In the Confirm Installation Selections screen, click **Install**.
9. Confirm that your installation complete successfully, and then click the **Close** button.
10. To verify that the web server has been installed correctly, at the browser address bar, type `http://localhost`. The default website opens and displays the IIS image.

Setting Up IIS on Microsoft Windows Server 2016

1. In the Start page, select **Server Manager**.
2. Select **Add roles and features**.
3. In the Before You Begin screen, click **Next**.
4. In the Select Installation Type screen, select **Role-based or feature-based installation** and click **Next**.
5. Click **Select a server from the server pool** with the current machine selected, and click **Next**.
6. In the Select Server Roles screen, check **Web Server (IIS)**. If a new window opens and prompt additional features are required, click **Add Features** to install, and then click **Next**.
7. Click **Next**.
8. Read the IIS information, and then click **Next**.
9. Click **Next** to install the defaults.
10. In the Confirm screen, review the install items, and click **Install**.
11. Once the set up is complete, click the **Close** button.
12. To verify that the web server has been installed correctly, at the browser address bar, type `http://localhost`. The default website opens and displays the IIS image.
13. Run FM Suite and select OHCFMSSecurityService as an added component to install onto the machine. A folder is created automatically with the same name OHCFMSSecurityService under `C:\inetpub\wwwroot` folder.

3

About Oracle Hospitality Cruise Fleet Management Viewer

Oracle Hospitality Cruise Fleet Management offers cruise operators industry-leading solutions with enhanced security, scalability, and functionality. All onboard transactions are automatically logged in real-time. Once a frequency is determined, this data is transferred to your cruise line's land-based offices for analysis.

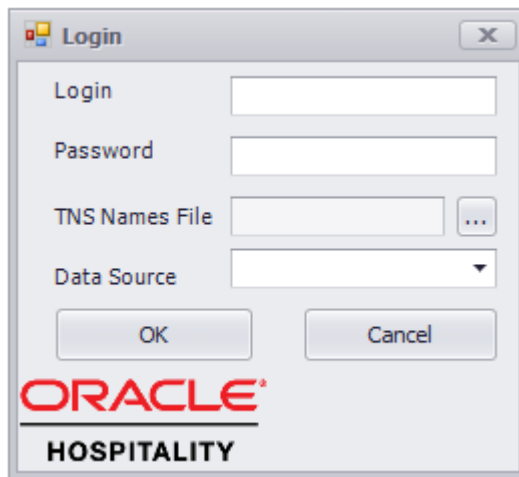
Oracle Hospitality Cruise Fleet Management contains the following features:

- Accurate and automatic data transfer from ship to shore
- Analytical tools for financial, marketing, and demographic analysis
- Shore excursion revenue analysis
- Availability of frequent cruise information across the fleet
- Guest data linked to the reservation system
- Real-time tracking of profit-and-loss performance at the head office

4

The FMS Login Screen

Figure 4-1 The FMS login screen

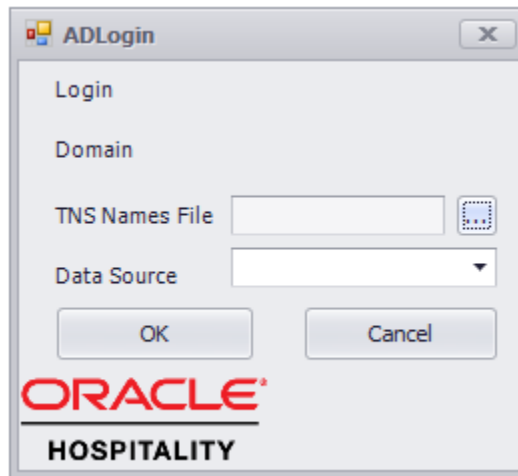


Login Screen for FMS Applications contains following fields:

1. **Login:** FMS user name.
2. **Password:** FMS password.
3. **TNS Names File:** Location for tnsnames.ora on user's system.
4. **Data Source:** Connect to the correct datasource.

Once you are validated, the Connection Key Manager screen appears for you to select a default schema. If you have selected a default schema earlier, the **TNS Names file** and **Data Source** are pre-filled with the user login after the validation application is launched.

Figure 4-2 The AD Login



Login Screen for FMS Applications contains following fields:

1. **Login:** AD user name.
2. **Password:** Domain password.
3. **TNS Names File:** Location for tnsnames.ora on user's system.
4. **Data Source:** Connect to the correct datasource.

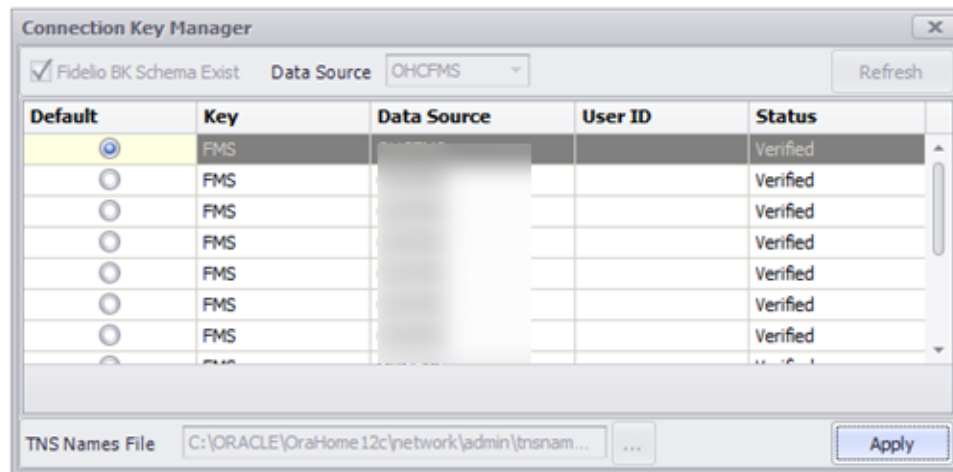
Once you are validated, the Connection Key Manager screen appears for you to select a default schema. If you have selected a schema earlier, the **TNS Names file** and **Data Source** are pre-filled with the user login after the validation application is launched.

To enable Active directory set "**IsActiveDirEnabled**" flag in App.config to "Y"

```
<appSettings>
...
<add key="IsActiveDirEnabled" value="Y">
</appSettings>
```

Connection Key Manager for FMS Desktop applications:

Figure 4-3 Connection Key Manager



You are required to select **Default schema**. **Data Source** and **TNS Names Files** are pre-populated from login screen and are non-editable. To start the application, click **Apply**.

Connection Key Manager for Sender/Receiver:

Figure 4-4 Connection Key Manager for Sender/Receiver

Config Settings

General

Root Path: C: [...]

File Retention Days: 7

Thread Pool Max Thread Count: 20

Mod Date Adjustment Hours: -3

SMTP Configuration

Server IP Address: [] Attach Error File

Server Port: [] Needs Authentication

Email From: [] User: []

Email To: [] Password: []

Email CC: [] Domain: []

Schema Info

Fidello BK Schema Exist Data Source: OHCMS1 Refresh

Default	Data Source	UserID	Status
<input type="radio"/>	[]	[]	Verified
<input type="radio"/>	[]	[]	Verified
<input type="radio"/>	[]	[]	Verified
<input checked="" type="radio"/>	[]	[]	Verified
<input type="radio"/>	[]	[]	Verified

TNS Names File: C:\Oracle\Oracle12c\network\admin\tnsnames.ora [...]

Apply

The selected **Default schema**, **Data Source** and **TNS Names Files** are pre-populated on login screen and are non-editable. To start the application, click **Apply**.

In the Connection Key Manager window, you can also configure the SMTP details and General Settings for Sender / Receiver

5

The FMS Dashboard

The Dashboard and the Fleet screens appear on your system start-up.

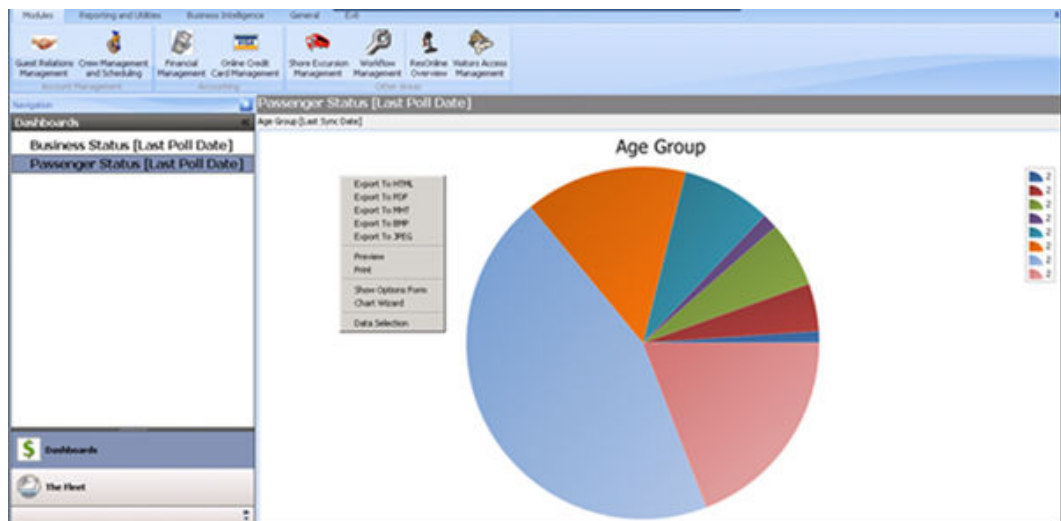
Dashboard

The Dashboard displays the daily data of ships. The revenue is grouped by financial classifications. The top 10 nationalities and the Age group chart represent the current status of guests onboard.

You can customize the Dashboard for individual login with the below steps.

1. Right-click inside the Dashboard and select **Show Customization Form**. Drag and drop the individual items to the Dashboard.
2. Save your customized layout.
3. Right-click inside the **Passenger Status [Last Poll Date]** window and export the details to other formats, such as HTML and PDF. The following figure explains the **Age Group** chart that represents the current status of guests onboard.

Figure 5-1 The Age Group Chart



The Fleet

The Fleet screen shows the itinerary of the ship in a calendar view and according to the branding. The ships are arranged according to their branding in the left pane. For example, all ships belonging to the default brand would show under Default. When you select the individual dates, the details about the passengers, crew, and the revenue for that selected date is shown.

Overview of Guest Relation Management

You can view and/or customize the guest details in the Guest Relation Management screen by:

- Guest Details
- Group Management

The following topics are available in this section:

Viewing Guest Details

1. In the Fleet Management screen, select **Module** menu, and click **Guest Relation Management**.
2. In the left navigation pane of the Guest Details screen,
 - a. In the **Search** section, enter **Passenger Info** in the given fields.
 - b. Click the **Ships** field and select the ship from the list.
 - c. Click the **Cruise** field and select the cruise from the list.
 - d. Select a port. Multiple port selection is allowed.
 - e. Click **Search** to search for the details. A list of ships appears in the right pane.
 - f. Select the ship of your choice and expand the list.
 - g. Select the guest from the list and the information is reflected in the extreme right pane.
 - h. Under **Embarkation/Disembarkation**, select the **Start** and **End** dates from the drop-down list.
 - i. Click **Search** on the lower left of the panel. The information appears on the right side.
 - j. Click **Port** to view the details of all the stored ports.
 - k. Search the **Date Range** from the guest embarked port to guest disembarked port.
 - l. Enter your frequent cruiser card information, under the **Card info**.
 - m. Enter the information in the given fields, under **Special Criteria**.

 **Note:**

Search criteria can work with any selection and it is not mandatory to choose the date and port together. You can also search by date and port individually and results are generated accordingly.

3. In the **Settings** section:
 - a. Select **Public** or **Private** settings.
 - b. Insert a template name and select **Save Current**.
 - c. Select an existing XML template in the **Load From** drop-down list.

- d. Click **Delete Current** to delete the template.

 **Note:**

If Private setting is selected, the template will only appear to the user who logged-in whereas the Public setting will show the template to all users.

4. From the **Grid Appearance** section, click the collapsible button and select the color of your choice to change the color of the screen.

 **Note:**

Not all onboard available Guest Details are shown on the **Fleet Management** screen, but these details are available for marketing data exports.

Viewing Group Management

Group Management is similar to the Guest Management screen. For more information about Guest Management, see [Viewing Guest Details](#)

Viewing Shore Excursion Management

Sales data and the number of guests attending the tour are shown on the Shore Excursion Management screen.

1. On the Fleet Management screen, select **Module** menu, and click **Shore Excursion Management**.
2. In the left navigation pane of the Excursion Setup Details screen, in the **Search** section, enter **Excursion** details in the given fields and click **Search**. The **Shore Excursion** details are displayed in the right pane.

Customizing Statistical Analysis

The Statistical Analysis screen provides financial data in form of pivot grids.

1. In the Fleet Management screen, select **Reporting and Utilities** menu, and click **Statistical Analysis**. The **Statistical Analysis** screen appears.
2. In the left navigation pane of the Statistical Analysis screen,
 - a. In the **Search** section under **Ship/Cruise**, enter information in the given fields.
 - b. Under **Demographics**, enter **Nationality**, **Age-Group** and **Gender**.
 - c. Under **Date Range**, enter **Start Date**, **End Date**, and **Fiscal Year**.
 - d. Under **Classifications/Departments**, in **Main Department** and **Sub Department** fields, enter **Group**, **Classification** and **Department** details.
3. Drag and drop the individual items from **Ship/Cruise**, **Demographics**, and **Date Range** into **Passenger Revenue Analysis** pane. The data are shown in the columns.
4. On **Statistical Analysis** screen, click **Department Analysis**. **Department Analysis** screen appears in the right pane.

5. You can rearrange the columns and rows in the **Department Analysis** pane.

 **Note:**

All the selected data from the various grids are visible in the form of graphical representation at the bottom of the screen.

6. To collapse or expand a list of Departments or Classifications, right-click anywhere in the Classification result shown in the **Department Analysis** pane, and select **Collapse All** or **Expand All**.
7. Select values in the grid and right-click the selection to export the details to other formats for example, .XLS, HTML, or PDF.
8. To use the Filter Editor, right-click the column header and click **Filter Editor**. The Filter Editor enables you to include a criteria filter.
9. In the **Settings** drop-down list:
 - a. Select **Public** or **Private** settings.
 - b. Insert a template name and select **Save Current**.
 - c. Select an existing XML template in the **Load From** drop-down list.
 - d. Click the **Delete Current** to delete the template.

 **Note:**

The Private settings only enable user who logged in to view this template. The Public settings shows the template to all users.

Exporting a Template

Data can be exported to a file for external data activities. There are two ways to export the data.

1. On the Fleet Management screen, select **Reporting and Utilities** menu, and click **General Utilities**.
2. On the General Utilities screen, click **File Export Utility**. **File Export** screen is displayed.
3. In the left navigation pane:
 - a. Select the **Template** from the drop-down list.
 - b. Select the **Type** from the drop-down list, select **Add Column Header** check box, and then click **Export**.
 - c. In the **Search** drop-down list, enter information in the required fields.
4. Select values in the grid and right-click the selection to export the details to other formats, such as *.XLS, HTML, PDF and so on.
5. To apply Filter Editor, right-click the column header, and click **Filter Editor**. Filter Editor enables you to include a criteria filter.

 **Note:**

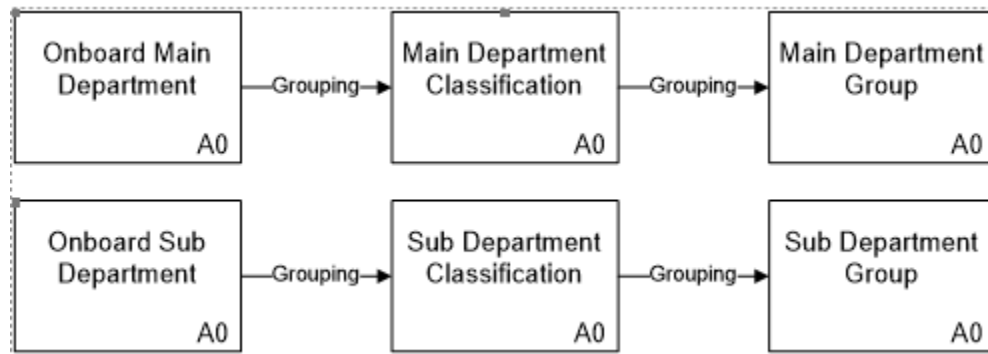
If you do not select any specific criteria in the search panel, by default, all the stored data gets reflected on the File Export screen.

6. Right-click the selected grid and select **Column Chooser** to customize your selection. Drag and drop the required columns into the **Customization** box.

Financial Classifications

Fleet Management System Financial Classification Setup enables you to group and analyze the data by classifying them into **Main** and **Sub department's** types, and have various departments grouped within each of the department types based on financial or unique similarities

Figure 5-2 Grouping of Main and Sub Departments



This data is further classified into two categories:

- Main Department - Group Classification
 - Main departments are grouped into main department classifications, and then to main department groups
 - Main department group (to be setup in FMS)
 - Main department classification (to be setup in FMS)
 - Main department of the individual vessel (as data transfer from the ship)
- Sub-Department - Group Classification
 - Sub-department are grouped into sub-department classifications, and then to sub-department groups.
 - Sub-department group (to be setup in FMS)
 - Sub-department classification (to be setup in FMS)
 - Sub-department of the individual vessel (as data transfer from the ship)



Note:

The main and sub-department hierarchy is separate.

Other Classifications

Other classifications enable you to group and analyze data on the cabin, category, sailing region base, and so on. Following are the current potential classifications and their descriptions:

Table 5-1 Classifications and their descriptions

Classifications	Descriptions
Cabin Classification	Special grouping for cabins could be: Inside, outside, suite, Crew, staff, officer.
Category Classification	Ships stateroom categories can be grouped to the advertised brochure cabin categories, such as Deluxe Suite, Standard A; B; C, and so on.
Cruise Itinerary Classification	The cruises can be grouped by its cruise regions following brochures releases or other analyzing criteria's, such as Europe, Mediterranean, Caribbean, Alaska, Baltic, and so on.
Cruise Season Classification	The cruises can be grouped by its cruise seasons following brochures releases or other analyzing criteria's, such as Fall 2009, Spring 2010, Summer 2010, Holidays 2010, Christmas 2010, and so on.
Excursion Classification	Excursions can be classified as requested analyzing criteria's, such as City tours, walking tours, half day, full day, or Low cost, high cost, and so on.
Maintenance Area or Location Classification	Areas for maintenance analyzing can be grouped fleet wise.
Maintenance Task Group Classification	Maintenance tasks can be grouped (higher level) and classified (lower level) for analyzing purpose.
Medical Item Group Classification	Medical sales items can be grouped (higher grouping level) and classified (lower grouping level).
Menu Item Group Classification	Menu sales items can be grouped (higher grouping level) and classified (lower grouping level).
Ship Category and Ship Classification	The vessels can be grouped by its ship category (holiday, rating category *****, and so on.) or by its ship classes (gross tons, Guest capacity, and so on.)

Setting Classifications Types

This topic describes how to set up and assigns Fleet Management System financial groups and classifications.

1. On the Fleet Management screen, select **Reporting and Utilities** menu, and click **General Utilities**.
2. Select **Classification Setup, Setup, or Classification Type**.

 **Note:**

The Classification Types are predefined.

Classification Assignment

The Main and Sub-department can be assigned to their respective Classification/Group using the drag and drop method.

1. On the Fleet Management screen, select **Reporting and Utilities** menu, and click **General Utilities**.
2. Select **Classification Setup, Assignment, Main Dept. Group** or **Sub Dept. Group**.
 - a. Select a ship. You can view the ship if the default radio button Ship view is selected.
 - b. Expand + next to **UNCLASSIFIED**.
 - c. Drag the departments from **UNCLASSIFIED** to the required department classification. You can select multiple departments by using the Shift key.
3. Click **Update All Postings**.

Once all departments are classified, the financial posting records (POS table) are stamped with the Classification ID and the Classification description.

Assigning Main and Sub-Department

1. On the Fleet Management screen, select **Reporting and Utilities** menu, and click **General Utilities**.
2. From **General Utilities, Setup, Classification**, select **Main Dept. Group** or **Sub Dept. Group**.
3. Right-click to add and assign a **Group** (Main or Sub) or **Classification** (Main or Sub).

 **Note:**

The classification should be linked to a higher lever Group under the Depend Type field.

Shore Side Departments

Data or information provided in Fleet Management is useful for corporate departments like Hotel Operations, Customer Services, Onboard Revenue, Finance, Marine Maintenance, Human Resources, and Marketing.

The following topics are available in this chapter:

Hotel Operation

The main areas of interest of a hotel operation are:

- Passenger data – Passenger listings per cruise/vessel/time period, including manifest data like Name, passport number, Date Of Birth, Guest picture, cruise and cabin details, address, flight details, etc.

- Guest history records (all cruises per individual Guest).
- Guest comments/complain data – per individual Guest and as analyzing summary per cruise/ship/fleet.
- Amenities and special request data.
- Medical records – individually per Guest, cruise/ship/fleet statistics. Possible medical fleet item classifications like Procedures, Medicines, X-rays (transactions, not images), Laboratory, etc.
- Onboard spending and invoice data - Guest checks and invoice details.
- Guest Comment Card data (cruise evaluation forms) – per individual Guest (image of scanned Guest card), analyzing, data comparison and charts per department, sailing, ship, fleet comparison.
- Work-order – per individual Guest/sailing and as analyzing summary.
- Guest group data – group, members, spending, and satisfactory level details.
- Financial performance per division – sales analyzing per sub-divisions like Housekeeping, Front Office using financial Fleet Management Flash Groups. Revenue reporting for selected departments only.
- House Account spending control - House Account, cruise, Guest check level.

Customer Service Department

For post-cruise customer service contact and/or analysis of customer satisfaction levels, the main areas of interest are:

- Guest Invoices, Guest checks - can be recreated (printed, exported to file) at any time directly within Fleet Management.
- Medical insurance invoices (Insurance claim forms) - can be reproduced (if initially issued onboard using medical module).
- Individual Guest comments and complaints - onboard follow-up taken, Guest compensations per Guest/cruise.
- Group records and account information.
- Guest and public areas maintenance Work-order - statuses, date and time of completeness.
- Credit card authorizations, settlements per Guest/cruise/transaction can be verified if transferred and required (details masked).
- Amenities and special request – verifying inserts.
- Guest history records (all cruises per individual Guest).
- Application activities – time of check- in, routing of posting, close accounts, etc.
- Gangway activities – verifying onboard presence during certain occasions.
- Individual Guest Comment Card ratings with included handwritten comments on the Comment Card.
- Complaint and work order statistics.

Onboard Revenue Department

The main areas of interest are analyzing onboard revenue by:

- Financial main and sub-department - by ship, ship class, cruise, fleet.
- Financial classification - main and sub-group, classification.
- Shore excursion - revenue analysis, per tour, port, country, excursion, demographics.
- MICROS item analysis – item count and revenue per item (cruise, ship, and fleet).
- Region analysis – revenue comparison of travelled region (Alaska cruises, etc.).
- Demographic analysis – revenues per nationality, age group, gender, etc.
- Back to back spending pattern – comparison of repeaters versus first cruiser.
- Group spending comparison, reporting.
- Revenue breakdown – average passenger per day, etc.
- Selective revenue charting.

This includes the creation and assignment of financial sub/main department groups/classification, item classifications, and excursion classifications.

Finance Department

The main areas of interest to management are the financial reporting and verifying financial reports, submitted by the ships as well as cash book and payroll data.

The main financial classification usually follows the corporate financial reporting grouping.

This includes creating and assigning financial sub/main department groups/classifications.

- Department Analysis – reporting by financial main and sub-department (cruise, ship, and fleet).
- Quarter Revenue Reporting – following the calendar quarters.
- Void journal controlling.
- Revenue reporting for Crew.
- Payment journals.
- Open balance reports.
- System account analysis.
- Cash book – reporting different currency cash books.
- Online Credit Card Management - CC authorizations, settlement, per Guest, cruise, ship, fleet, type.
- Payroll Overview and Reporting

Marketing Department

It is possible to review customer revenue-behavior and feedback based on demographics (nationality, gender, age mix/profile). The main areas of interest are:

- Guest onboard spending based on demographics.
- Spending analyzing per department and demographics.
- Guest Comment Card summaries (if the Comment Card module is used).

Includes cruise classification, cruise region classifications, and category classifications.

Adding and Editing a Ship

The section describes how to configure a new ship or edit an existing ship details in Fleet Management Viewer.

1. On the **Administration** screen, click **Ship Setup**.
2. Select **Details** and then select **Fleet Management**.
3. Fill in the following details in **Ship Details**:

Table 5-2 General properties for Adding a Ship




Properties	Description
Status	Select the status as Active/Dry Dock/Inactive . By default, the status is Active. This is a mandatory field.
Ship ID	Enter the ship ID. The ship ID should be between 11 and 98. The Ship ID must be unique and if duplicated, gives an error. This field is mandatory.
	<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;"> <p> Note: This field is enabled only in the Add mode. Right-click to edit this field.</p> </div>
Ship Name	The Ship Name of the selected ship gets automatically displayed.
Ship Short Name	The Short Name of the selected ship gets automatically displayed.
	<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;"> <p> Note: This field is enabled only in the Add mode. Right-click to edit this field.</p> </div>
Company Name	Enter the name of the company. The maximum length is 50. A pre-filled list of existing distinct values of this column can be displayed for selection. If you want to enter a new value, type the value. The status is enabled always and this field is not mandatory.
Classification	Select the Classification from the drop-down list.
Category	Select the Category from the drop-down list.
Security Class	Shows the default.

Table 5-2 (Cont.) General properties for Adding a Ship

Properties	Description
Ship Image	Shows the image of the ship.
ERS status	Select the Emergency Response Status as Yes or No . The default status is NO . If you select Yes , you are setting frequent data transfer from ship to shore.

 **Note:**
This option should be enabled in case of Emergency only.

- In the **Selected Ship Partitions List**, select only the tables.

 **Note:**

Green color signifies the tables exist, and red color signifies the tables does not exist.

- Click **Save** and click **Yes** to continue.
- In the left navigation pane, under **Ship Selection**, right-click the ship you need to edit. Do the required changes and the data is edited and saved in the database.

Change Logs and Error Logs Details

- On the Administration screen, click **Ship Setup**.
- Select **Change Logs** or **Error Logs**.
- Under **Ship Selection**, select the ship. The data is displayed on the Change Logs or Error Logs screen.

By default, the results are populated with date and time and in descending format.

Following is the column description for Screen Change Logs and Error Logs:

Table 5-3 Column description for Change Logs and Error Logs

Column	Description
Procedure Name	Ship Insert/Update/ with schema name.
Log Details	Displays the detailed log of what activity is performed by the Admin.
Changed By	Displays the User ID of the logged-in user.
Changed Time	Displays the date and time of the changed log and the time of the error.

Adding Users and Groups

User authorization privileges are configured within the Fleet Management Administration module. Fleet Management uses an authorization mode where each user belongs to one or more user groups, and then the user gets all the privileges assigned to the user group(s). Alternatively, Fleet Management can use Active Directory as an alternative for authentication/authorization. In the Active Directory mode, the Microsoft Windows user is used to login into Fleet Management.

To add Groups and Users to the Cruise Fleet Management System:

1. To create a group:
 - a. On the Fleet Management System screen, from the **Administration** menu, select **General**.
 - b. On the **Administration** screen, click **User Security** and then click the **Group**. On the left panel under Groups, right-click any group and click **Add**.

After selecting the information for the group and the user rights, click **OK** to save. The administrator can select the various modules to create groups.
2. To create a user:
 - a. On the **Administration** screen, click **User Security**. On the left panel under **Groups**, right-click any of the group and click **Add**.
 - b. Enter the **User Login**, **Password**, **First Name**, **Last Name**, **Group**, and **Class**. You can enable or disable the user by selecting the **User Enabled** check box.
 - c. Select the drop-down list of the group section and then click **OK**.

Logging And Security Shore-Side

In Fleet Management System, users are assigned rights based on their department/group. The departments can be Finance, Operations and Administrators, and rights that are assigned to them. Access rights are assigned based on group and users can be allotted within them, thus maintaining a filter of access. Groups that are part of Administrators will have full access rights. In the case of an invalid user name or password used at log in, a warning will appear on the screen. The user is locked out on the seventh (7th) attempt for five (5) minutes if incorrect credentials are entered.

Fleet Management System has a dedicated screen that logs the users' access to different modules and applications, which shows the details of users and the activity they performed on the application including the date, workstation, OS User and user name.

Logging In FMS Database Shore-Side

Logging into Fleet Management System Database Shore-Side explains the Activity Logs of the logged-in user.

- The user's access log to different modules in Fleet Management System application is stored in the **ACTIVITY_LOG** table in **FCFMSADMIN** schema in the database.
- The **ACTIVITY_LOG** table logs in all activities of the user in the FMS System. These details can also be viewed from the FMS Activity Log Viewer function.

- Each DDL activity performed is recorded in the FIDELIOBK.DDL_AUDIT table.
- FIDELIOBK.DDL_AUDIT table capture activities like CREATE, ALTER, DROP, RENAME OR TRUNCATE ON SCHEMA.

Active Directory Integration In Fleet Management System

Active Directory is activated by changing a parameter in the database. The parameter table has a Y/N flag as PAR_VALUE within the Group. When the parameter is set to Y, the Active Directory is integrated with Fleet Management System. The integrated Active Directory function in the following manner:

- Upon start-up the application fetches the active directory information of the OS user.
- Once the user is authenticated by the active directory, only then they can access the application. If the authentication is not done, then the application closes after giving a message.
- The active directory connection details are logged once the Active Directory authentication is done. The details logged are date, user, domain, email, group, and workstation.
- If User Groups do not already exist, then they are added to the User Groups of the Active Directory.
- The Operating System user gets the rights assigned to the Active Directory Groups within the application.

Setting up Active Directory

To set up an Active Directory:

- Identify the users who must have administrator privilege in the Fleet Management System Application.
- Ensure all such users belongs to the same domain.
- Notify the exact domain group name for administrator rights so that we can set them up.
- Once privileges are granted in Fleet Management System, the domain group users can try running the Fleet Management System from their domain group logged- in machines.
- Any user of the domain with administrator privileges can grant or revoke privilege to users of another domain group.
- All user privileges are based on domain group, hence any user belonging to a domain has the same privilege as members of that domain group.
- A user belonging to more than one domain group would have the privilege that are union of both domain group.
- Once a user from any new domain group logs in; their details are automatically entered in required tables.
- The administrator user from the Administrator group as identified above can then give desired rights by right-clicking on the domain group and selecting edit.

6

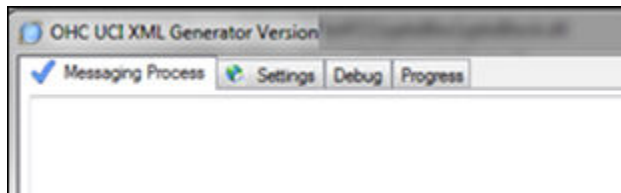
Universal Check In XML Generator

The Universal Check In XML Generator creates the Extensible Markup Language (XML) from the checked-in passengers data of the cruise.

Messaging Process

Universal Check In XML Generator shows the messages that are being processed on the Messaging Process screen.

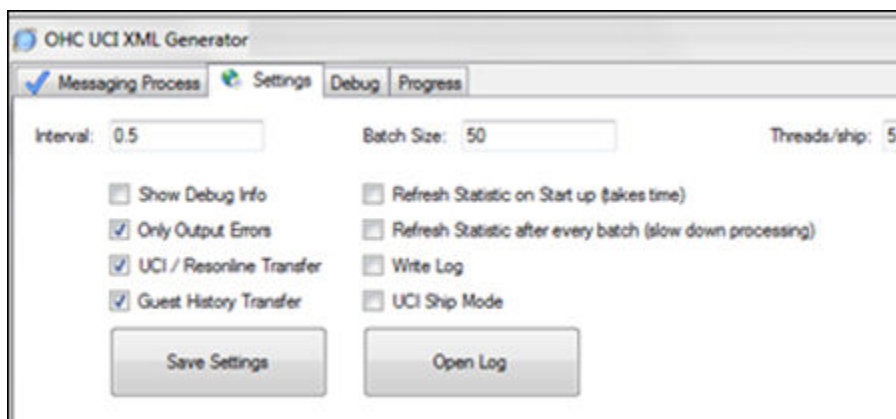
Figure 6-1 Universal Check In XML Generator



Settings

This section defines the required settings for Universal Check In XML Generator.

Figure 6-2 OHC UCI XML Generator



7

Database Schema Password Manager

The Database Schema Password Manager is used to:

- Migrate schema entries to the latest encryption.
- Change schema passwords to allow the ownership of passwords to be with the customers.
- Add new schema entries.

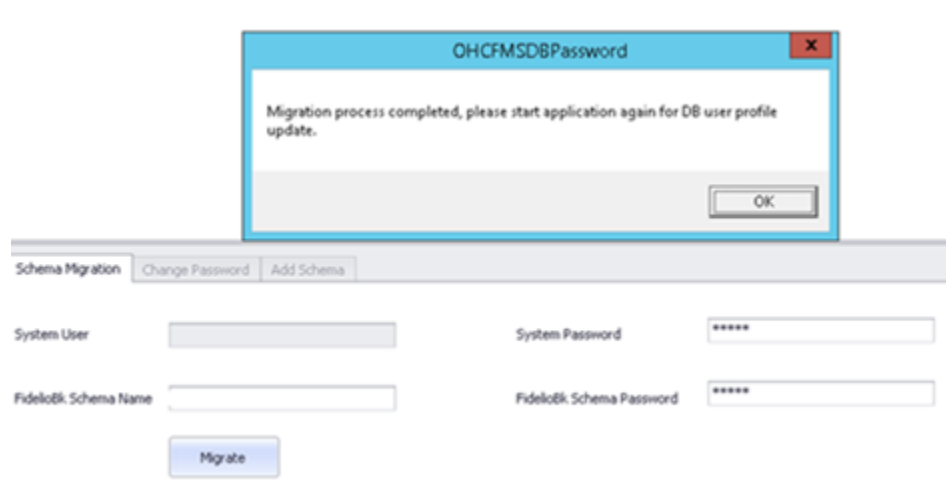
Migrating Schema Entries to the Latest Encryption

Schema Migration is the first tab of the Database Schema Password Manager. This tab is used to migrate the Non-PADSS or OLD PADSS encrypted password entries to the most recent encryption; therefore, the tab is only enabled if an entry is using OLD PADSS or NON PADSS encryption. If the schema has all entries on the latest encryption, this tab is not enabled.

To migrate schema entries to the latest encryption:

1. Enter and save **OHCFMSSecurityService.url** and **AdminModeDataSource** (data source name) in the `FCDBPassword.config` file.
2. Click the **Schema** tab, and then enter the following information:
 - **System User:** Enter the database system user name.
 - **System Password:** Enter the system user password.
 - **Schema Name:** Enter the schema name.
 - **Schema Password:** Enter the new password for the schema.
3. Click the **Migration** button to proceed.
4. Click **OK** to complete the migration.

Figure 7-1 Schema Migration tab in the Database Schema Password Manager screen

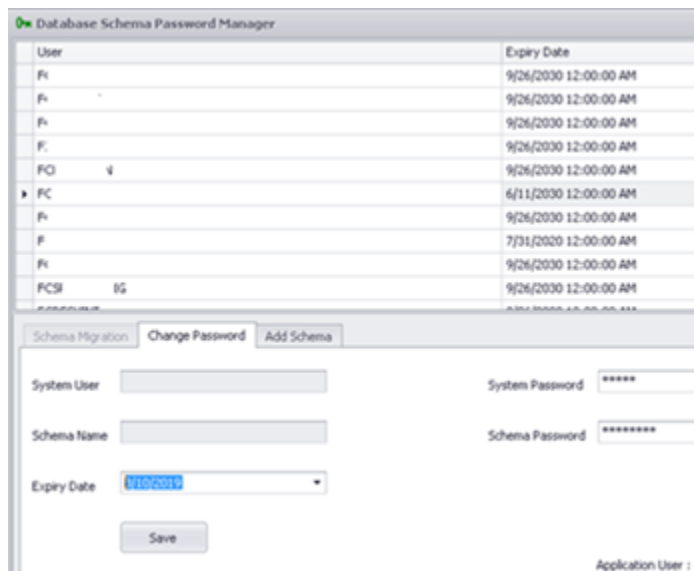


Changing Schema Passwords

The Change Password is the second tab of the Database Schema Password Manager. This tab is used to provide ownership of passwords to customers.

To change a schema password:

1. On the Database Schema Password Manager screen, select a schema you wish to change the password.
2. Click the **Change Password** tab, and then enter the following information:
 - **System User:** Enter the database system user name.
 - **System Password:** Enter the system user password.
 - **Schema Name:** This is automatically populated with the schema name and is greyed out.
 - **Schema Password:** Enter the new password for the schema.
 - **Expiry Date:** Enter the new expiration date.
3. Click **Save** to complete the password change.

Figure 7-2 Change Password tab in the Database Schema Password Manager screen

Adding a Schema Entry

Add Schema is the third tab of the Database Schema Password Manager. This tab is used to add a new schema entry to the FIDELIOBK schema.

To add a new schema entry:

1. Click the **Add Schema** tab, and then enter the following information:
 - **System User:** Enter the database system user name.
 - **System Password:** Enter the system user password.
 - **Schema Name:** Enter the name for the new schema entry.
 - **Schema Password:** Enter the password for the new schema.
 - **Expiry Date:** Enter the expiration date.

Note:

The latest encryption key is used for new entries.

2. Click **Add User** to complete the addition of a new schema entry.

Figure 7-3 Add Schema tab in the Database Schema Password Manager screen

Database Schema Password Manager

TNS Names File C:\ ... Connection Name

User	Expiry Date
FC	6/1/2019 12:00:00 AM
FC	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM
F	6/1/2019 12:00:00 AM

Schema Migration Change Password **Add Schema**

System User System Password

Schema Name Schema Password

Expiry Date

Existing Encryption Key will be used to encrypt password

Add User

8

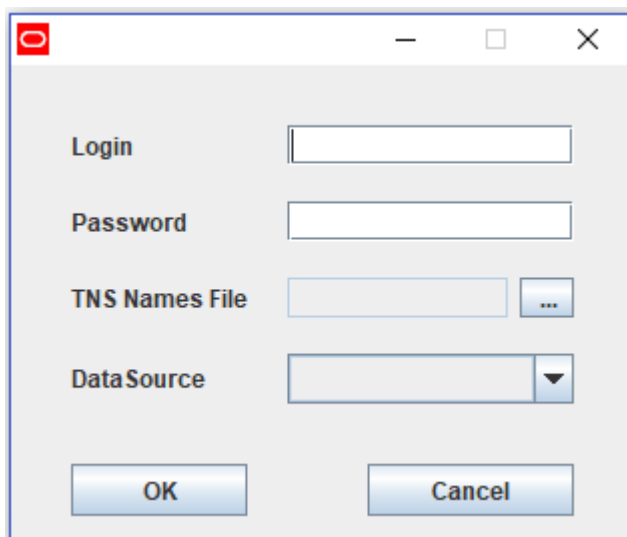
Database Updater

DBupdater is a tool that run and update the database using scripts. When the DBupdater is installed, follow the below settings to allow DBupdater to run.

1. In Environmental Variables, enter TNS_ADMIN as environment variable name and the variable value is the path to Network folder of ODAC).
2. Your TNS file must be placed in the admin folder.
3. Copy the scripts into the script folder.
4. Add the scripts sequence in Sequence.txt.
5. Modify `project.properties` file, which is placed under the Config, to update the ServiceURL for OHCFMSSecurityWebService.

Database Updater Login Screen

Figure 8-1 The Database Updater Login Screen



1. Enter your FMS username.
2. Enter your FMS password.
3. Browse the tnsnames.ora location on your system.
4. Select the datasource that you want to connect.

When you are successfully validated, the system will access the main screen.

Figure 8-2 Establish Connection screen



The **Run Scripts** button will only enable when you enter a valid credential. Once logged in, you can select the scripts you want to run followed by **Run Scripts**.

9

Corporate Data Transfer Interface

The Corporate Data Transfer Interface (CDTI) provides a mechanism for transferring data to external systems outside of customer domain to other vendors too. It is based at shore-side location and uses the Fleet Management database. This interface is flexible and dynamic and enables the shore-side user to modify settings to provide formatted/customized solution.

Methods of Data Transfer

The following methods of data transfer are available:

- Transmission Control Protocol/Internet Protocol (TCP/IP) Connectivity - This method allow the external system to establishes a direct connection to the Corporate Data Transfer Interface (CDTI), and on the Listener port as and when required and poll data based on pre-agreed messages. The external system would also open a listener port which allow the Corporate Data Transfer Interface (CDTI) to send any triggered messages. This method sends a full record in one message.
- Flat File Transfer - Enables you to assign a pre-agreed folder as the location to place the files whenever it is scheduled to do so.
- Microsoft Message Queuing - This method is provided on-demand, only if the external system can work with Microsoft Message Queuing (MSMQ). If it is, then messages are transferred over Microsoft Message Queuing (MSMQ) to a pre-defined queue with the structure being exactly similar to that of the Transmission Control Protocol/Internet Protocol (TCP/IP) Connectivity. In this method, one message contains one full record only.
- Web Service- This method allows you to call web service methods periodically using the required parameters.

In Exporter, data transfer is done through File transfer and web service. In Importer, data transfer is done through TCP/IP, MSMQ.

Message Formats

The following message formats are available:

- Extensible Markup Language (XML) format - This follows the Extensible Markup Language (XML) Schema 1.1 standard. This method is available in all three methods of data transfer.
- Delimited Flat File - This method enables the Corporate Data Transfer Interface (CDTI) to throw an output in tab-separated values (TSV), comma-separated values (CSV) or any other user-defined delimiting character. This method is available only in the Flat File data transfer.
- Fixed Length Flat File - This enables the Corporate Data Transfer Interface (CDTI) to write output in a pre-defined fixed length for each column in the transfer. This method is available only in the Flat File data transfer.
- JSON Format –This format is used for web service integration only.

Types of Data Transfer

The following types of data transfer are available:

- **Triggered Messages** - These are messages that the Corporate Data Transfer Interface (CDTI) sends automatically to the external system whenever an event is triggered. This could be when a particular cruise is closed in the cruise table or after a certain time of the cruise closing, to ensure all data from the ship has transferred completely from the ship to shore. This method supports all three data transfers.
- **On-Demand Messages** - These are pre-defined messages that the external system sends to the Corporate Data Transfer Interface (CDTI) and gets an answer in a pre-defined format. This method only supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Microsoft Message Queuing (MSMQ) transfer methods.

Type of Connections

The Corporate Data Transfer Interface (CDTI) enables you to define multiple connections, both Inward and Outward. The Inward connection receives message requests and the outward connection sends the responses. The following are the types of connections available :

- **Inward Connection** - There are two types of Inward connections you can use - Transmission Control Protocol/Internet Protocol (TCP/IP) and Microsoft Message Queuing (MSMQ). On the Transmission Control Protocol/Internet Protocol (TCP/IP), you can define the port that the Corporate Data Transfer Interface (CDTI) should open and listen. On the Microsoft Message Queuing (MSMQ), you can define the name of the Private Queue on the local machine that the Corporate Data Transfer Interface (CDTI) should poll regularly.
- **Outward Connection** - You can define, as many Outward connections as there are external systems. One External system can also have more than one Outward Connection. The Outward Connections can also include the Flat File Transfer.

Message Structure

The Corporate Data Transfer Interface (CDTI) can handle many messages. These messages are definable through the Corporate Data Transfer Interface, providing you the flexibility dynamically. The following is an example of message structure.

```
Request:
<?xml version=1.0 standalone=yes?>
  <request>
    <shipid>SHIP_ID</shipid>
    <sailingdate>SAILING_DATE</sailingdate>
    <guestid>GUEST_ID</guestid>
  </request>
Response:
<?xml version=1.0 standalone=yes?>
<response>
  <shipid>SHIP_ID</shipid>
```

```
<sailingdate>SAILING_DATE</sailingdate>
<guestid>GUEST_ID</guestid>
<type>Passenger Reservations</type>
<cancel>N</cancel>
<booking>
  <personalinfo>
    <firstname>Name</firstname>
    <lastname>LastName</lastname>
    <dateofbirth>DATE_OF_BIRTH</dateofbirth>
    <gender>PASSENGER_GENDER</gender>
  </personalinfo>
  <passportinfo>
    <nationality>Country</nationality>
    <passportno>PASSPORT_NO</passportno>
    <passportissuedate>PASSPORT_ISSUE_DATE</passportissuedate>
    <passportissueplace>PlaceofIssue</passportissueplace>
    <passportexpirydate>PASSPORT_EXPIRY_DATE</passportexpirydate>
  </passportinfo>
  <cabininfo>
    <cabintype>CABIN_TYPE</cabintype>
  </cabininfo>
</booking>
```

10

Watchdog

The use of Oracle Hospitality Cruise Watchdog enable you to restart the application at predefined time without having to manually login whenever it restarts.

Watchdog, will start and refreshes the interfaces added, enabling its WatchdogRule file and silently authenticate with the latest available login screen.

You are advised to install and configure the Watchdog application in FMS 9.1 for silent authentication when you restart FMS, if it is not already running on the machine. This is only applicable to Interfaces Sender, Receiver, ResOnline, and ResOnline Polar.



Note:

Failure to install and configure Watchdog may cause a record processing delay.

Adding a New Rule

For each application, the rules need to be defined separately.

1. From the Fleet Management Watchdog Service Status screen, click **Add**.
2. The new Rule is highlighted in the left column. Click **Edit**.
3. Enter the details about the application, such as **Rule Name**, **Rule description**, or **Executable**. Check or uncheck the **Actions** (i.e. Conditional Restart Action, Scheduled Restart Action and Run Instance Action).
4. Click **Apply** to save the Rule.

11

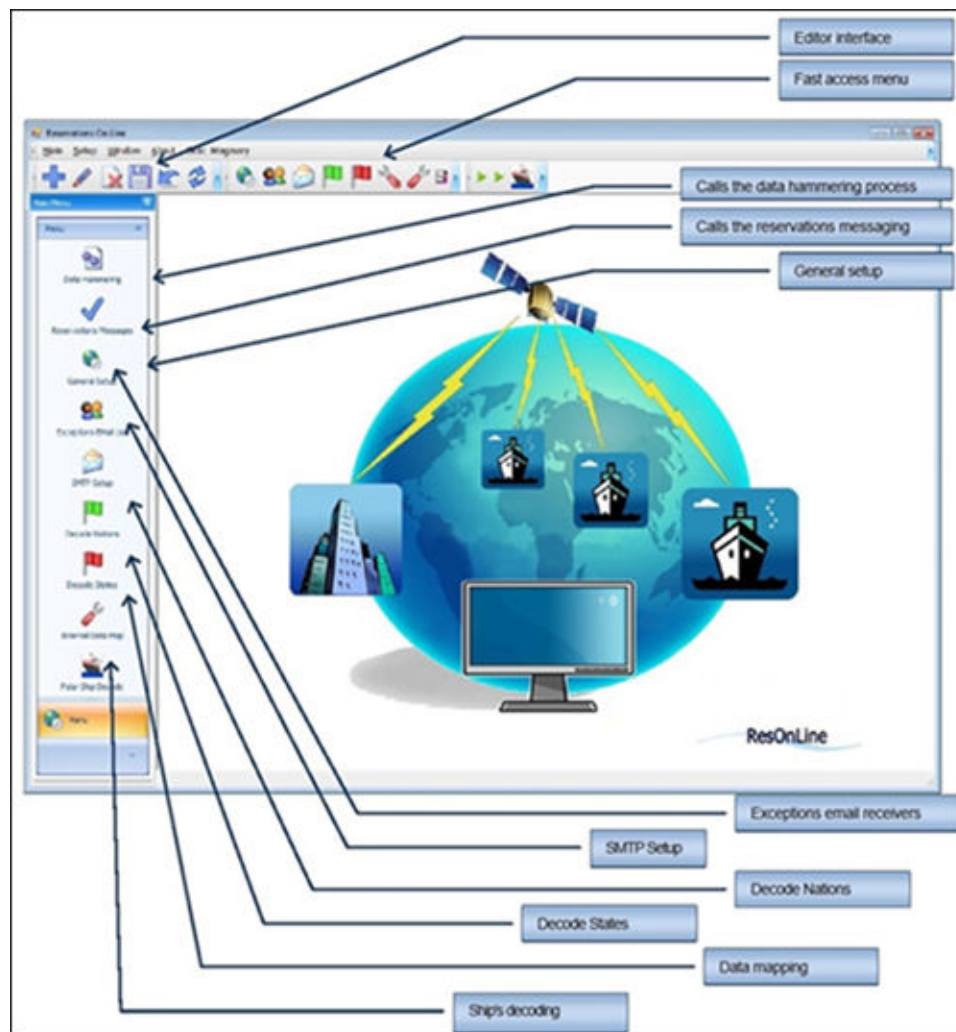
Reservations Online

The Reservation Online module ensures the data gets transferred from the reservation system to the ship side without any manual intervention, and this would require fields to be mapped for accuracy. See [Document ID 2575588.1 Oracle Hospitality Cruise Fleet Management OHC ResOnline to SPMS Mapping and Specifications](#) for more information.

The standard and the main responsibilities of this module are:

1. Homogenize the otherwise distinct source data from the external reservation systems and render it compatible with the SPMS data structures.
2. Compose the entire passenger's reservation into a composite business object entity and deliver it to the corresponding vessel within the correct deliverable date range.
3. Repository for audit activities from FMS.

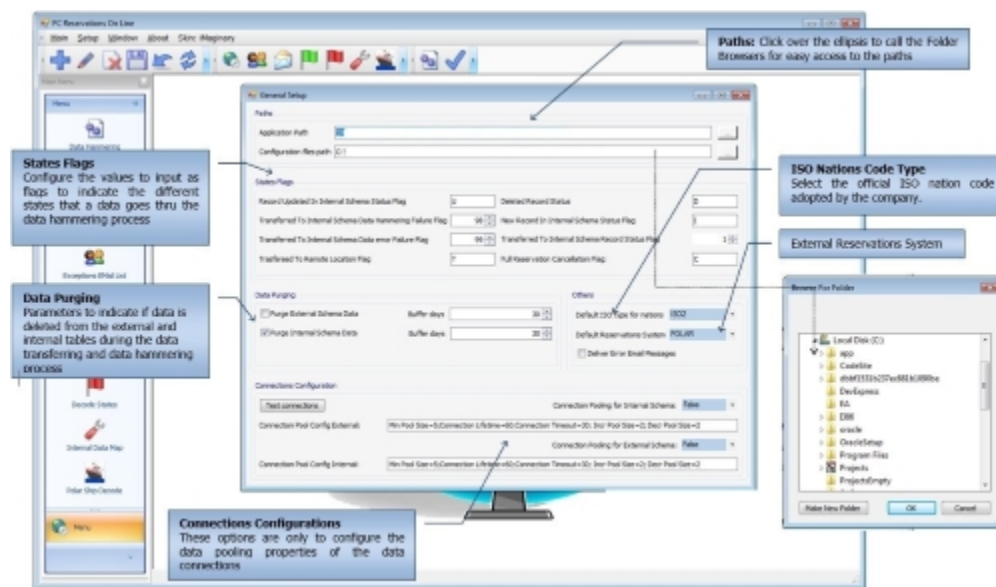
Figure 11-1 Cruise Reservations Online



General Setup

This section explains the setting up of general parameters like the data path , data transition states flags, and others.

Figure 11-2 General Parameters



Reservation Online application logging has two logs files:

1. ExceptionLog.txt
2. Log.txt

The ExceptionLog.txt files are backed up with date-time stamp once it reaches 5MB size, and Log.txt file are overwritten.

Ships Decode

This set up is needed to convert ships code from Polar to the equivalent FM codes. Also, it enables you to assign several sets of ships to different processing machines for load balancing. Some sections of the vessel decoding are for the main Reservation Online application use only.

Figure 11-3 Ships Decode set-up

Use the standard bar to Add, Delete or Edit ships.

This is the vessel code that arrives from Polar data, which will be decoded to the FMS Ship Code.

Click here to assign the selected ship to the machine. If the selected ship was already assigned to another machine, click twice to clear and re assign it. You can set this up in the ResOnLinePolar but the filtering is used only by the main ResOnLine application in the Data Hammering process.

This value is used to calculate the date range from which all the reservation will be delivered to the vessels. In this case the range will be calculated by today's date plus 22 days.

You have the possibility to assign different values for each one of the ships.

You can set this up in the ResOnLinePolar but the filtering is used only by the main ResOnLine application in the Messaging process.

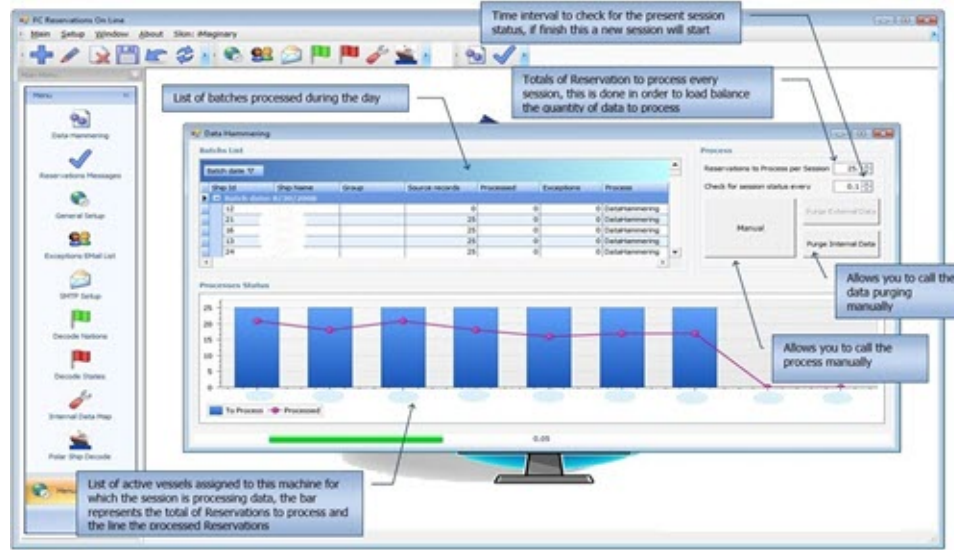
The short name is used by the charts in the main ResOnLine application

Ship Name	Source Code	FMS Ship Code	Assigned To Machine	Short Name	Status	No. Days for Data
A	24				INACTIVE	22
D	24				ACTIVE	22
E	17				INACTIVE	22
H	17				INACTIVE	22
N	22				INACTIVE	22
O	21				INACTIVE	22
P	11				ACTIVE	11
S	12				ACTIVE	22
T	15				INACTIVE	22
U	20				INACTIVE	22
V	18				INACTIVE	22
W	22				INACTIVE	22
X	19				INACTIVE	22

Data Processing

During Data Processing, the application gathers records from the external source and proceeds to insert or update corresponding records in the target tables as configured in the data mapping. This process proceeds the data in the way the Reservation Online can deliver the data to SPMS.

Figure 11-4 Data Processing



To process credit card data, you need to have both the SPMS and FMS Key pair.

See [Encryption Manager](#) section for more information.

Source Data Filtering

When processing the source data such as Passenger's Air flights, different types of addresses, Special Requests, or Gift Orders, the application needs to filter only the specifically required data from the same source.

A logical target column called **DATA_FILTERS** enables you to create a combination of data filtering rule for each one of the source and target that requires it. For example, the first record combination instructs the application to extract only flights data where the source field **PAX_CARRIER5** is not empty when processing data for the target table **FLIGHTS** and detects that the source fields set contains the field **PAX_FROM_AIR5**

See topic [Reservations Online](#)

Reservations Messaging Process

This process select the records from the internal schema that stores the transformed reservations data processed before, and then converts the data into an XML message that is delivered to the respective ships by FMS Sender and Receiver.

Once the left panel is visible, you can view all the messages and their respective XML text by scrolling the batch list.

Interface - Import Reservations To The Ship Database

To send and receive reservations and statuses, FMS Sender/Receiver and MSMQ are used alongside with the OHC DGS ResOnline interface for data import to SPMS. This

interface imports reservation provided by FM Transfer, and then sends back a status for each record to the shoreside.

Reservation Status

The FMS Reservation Online module controls the dataflow status.

Table 11-1 FM Reservation Online module

Status	Description
Passenger Manifest	Shows all reservations imported and processed, together with their ship import statuses.
FM Dashboard ResOnline Transfer Status	Provides quick data of how many reservations we currently have to send per ship and how many have status Pending (not processed onboard yet).
Transfer Status	Detailed grid shows how many reservations were loaded, processed, transferred, imported and pending.
Loading Status Grid	External files upload status. Provides an overview of daily upload process.
Ship Response Messages	Allow seeing the complete ship import history of each individual reservation.
Reservations Status SPMS Viewer	In SPMS, provides an overall history status on daily basis - what is new, updated, deleted.
Reservations Status SPMS Reports	In SPMS, provides a status report.

Reservation Status Alerts

Reservation Online sends alerts and email transport protocols. There are two groups of alerts, each with different distribution lists and destinations (ship/shore departments):

- Emergency
- Status alerts

12

Sender and Receiver Data Transfer Interface

The FM Transfer Interface is an interface that transfers data dynamically between the ship and shore side repository. It uses Microsoft Message Queuing (MSMQ) as a basis for its transport mechanism. The Interface is comprised of two components:

- Sender
- Receiver

The Interface is very complex and changing any of its settings arbitrarily could result in data not transferring across successfully. It is therefore recommended that Oracle Hospitality Cruise is informed before making any serious changes. Among changes to coordinate are: moving the Interface to another computer, changing queue names, changing the operating system (OS) of the computers, running the Interface, or modifying the transfer setup in **FMS_TRANSFER** table.

Also, note that increasing or decreasing the Batch Size for different tables or the Thread counts should not be done merely because the option exists. Its settings are based on a lot of testing and changing these could result in longer transfer times, bottlenecks on the satellite and exhausting the resources of the computers running the Interface or the Database Server. Furthermore, Oracle Hospitality Cruise recommends that even general setup changes from within the Interface should be coordinated and carried out by one designated person for the whole fleet.

When setting up the interface, do take into consideration the use of Mod Date Adjustment Hours described below which apply to both the Sender/Receiver Data Transfer.

MOD DATE ADJUSTMENT HOURS: This is a negative number defining the number of hours that overlapped from the last transfer date and time. When the daily scheduled transfer takes place, it picks up data that has been modified since the last transfer date for each table it has to transfer. So if the last transfer time was at 04:00 hrs of the previous day, the Interface picks up all data was modified from 01:00 hrs of the previous day. This accommodates most scenarios involving time changes, modifications done during transfer.

Configuring Sender

1. Go to `C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS Sender`.
2. Open `OHC FMS Sender.Config` file and update the `ServiceUrl`.
3. Set the flag **Y/N IsActiveDirEnabled**.
4. Set the flag **Y/N isShipSide**.
5. Then save the settings.
6. Set the **TNS Names File** and the **Data Source**.
7. Then login with your user name.
8. Select the appropriate schema name.
9. Click **Apply** to save the settings and launch the FM Sender application.

10. Click the settings tab, select the desired destination.
11. Right-click the Queue Info window and add a new Queue.

The settings are saved in an XML file called ConfigSettings. The password is saved in a 128 bit encrypted form. You can always modify these settings by clicking on the **Config Settings** button under the **Settings** tab of the OHC FMS Sender.

See [Table 12-5](#) for fields definition.



Note:

You must restart the interface for the settings to take effect if you modify any of the settings or add new queue entries.

Activity Status

The Activity Status shows the activity status of Fleet Management Sender.

Table 12-1 Activity Status

Activity Status	Description
Direction	The transfer tables are divided into various groups for ease of transfer settings. Each direction above shows a different set of tables. The settings of tables are explained later in the Settings tab.
Status	The status of the direction group that is being transferred.
Last Transferred Date	The last date on which the data was transferred for that Direction Group.
Next Transfer At	The next scheduled date and time on which the next transfer would take place for that Direction Group.

Table 12-2 Columns of the Data Grid

Columns	Description
Destination	Receiving end of the transferred data.
Direction Group	The direction group of data that is being transferred.
Ship	Ship number.
Table	Table that is being transferred from the visible direction group.
Transferred On	Date along with time on which the table is transferred.
Batch	Each transfer table is divided into batches for transfer. The batch number getting transferred and the total number of batches shows up here.
Records	The number of records transferred of the batch.
Remarks	Any error/warning or remark of the batch being transferred is shown.

**Note:**

The other tab shows the **Log reader** of the Sender is used for debugging by the support team.

Settings

The settings tab shows direction groups, their transfer timings and MSMQ (Microsoft Message Queuing) level information. Direction groups can be added/edited and configured from here.

Table 12-3 Direction Groups

Name	Description
ShipToShore	Selection of tables that need to be transferred once a day. Set to transfer at 5 AM daily.
Setup data	All tables requiring transfer more than once a day. For example, table that gets changed frequently and /or impact the business. Set to transfer every 3 hours.
Lob data	All tables with Blob/picture fields are transferred separately as they take more time to transfer. They are also set to transfer once a day. Set to transfer at 6 AM daily.
Trans-tables	Contain the settings related to transfer tables. These tables are used by support team for investigation problems. Set to transfer at 8 AM daily.

Config Settings

This setting allows you to change the settings such as SMTP or schema info.

To modify the config settings, click the **Settings**, then **Config Settings**. The General settings are thread level settings of the interface.

SMTP Configuration: The Sender can send out alerts in case of errors and in case of inactivity. You can enable this feature by filling in the following SMTP details:

Table 12-4 SMTP Details

SMTP Details	Description
Server IP Address	IP address of the email server.
Server Port	The default is 25. Change if it is different for your mail system.
Email From	From identifier of the email sender. For example, Test FM Sender.
Email To	Email address of the receiving group/person.
Attach Error File	Checking the Attach Error File would attach the error file to the email and the email would be sent to the defined email addresses.
Schema Info	Gives the information of the database schema sender is sending data from.

Setup and Configuration

Microsoft Message Queuing (MSMQ)

The Interface sends messages over MSMQ in compressed and encrypted packets. The responsibility of successfully delivering the packet to the destination queue lies within the MSMQ architecture, which in turn relies on the network connectivity provided between the source and destination. Since ships send data over satellite and this connectivity may drop at any time, MSMQ holds the messages at the source until it re-establishes connectivity and then sends it across, thereby ensuring a successful transfer of every packet.

The Interface transfers data in two modes:- Workgroup and Active Directory (AD). Active Directory mode is a secure mode where messages are encrypted and authenticated using the certificates on the Domain Controller.

 **Note:**

AD mode requires installation of MSMQ on the Domain Controller. It only works if the Sender and the Receiver machines are in the same domain.

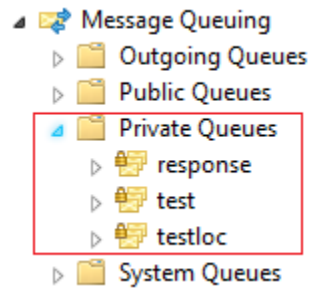
The MSMQ component needs to be installed on every machine that runs OHC FMS Sender/Receiver . Since it is NOT installed by default, it has to be installed later from the Windows Components under **Add/Remove Programs**. During the installation process, make sure ALL sub controls of MSMQ are installed, and you must select *Integration with Active Directory* if the data transfer in AD mode is required.

A typical one-way communication requires the queues to be created only on the Receiving end, logically this would imply shore side. But if the solution requires a two-way communication, a queue also needs to be created onboard to handle any messages coming in. At the shore side, a queue should be created for each ship.

MSMQ Settings in Workgroup Mode

To create a queue in the **Workgroup Mode**, go to **Computer Management**, select **Services and Applications**.

1. Expand Message Queuing and right-click **Private Queues**.
2. Select **New, Private Queue**. The queue is to remain as non-transactional.

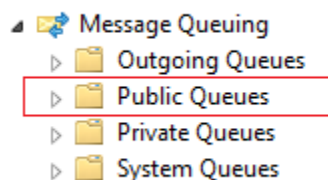
Figure 12-1 MSMQ Private Queue List

The local computer or the domain user can run the Sender/Receiver in workgroup mode and create Queues to send or receive data using private queues. Additionally, user is required to create a response queue to receive responses from data transferred.

MSMQ Settings in AD Mode

To create a queue in the **AD Mode**,

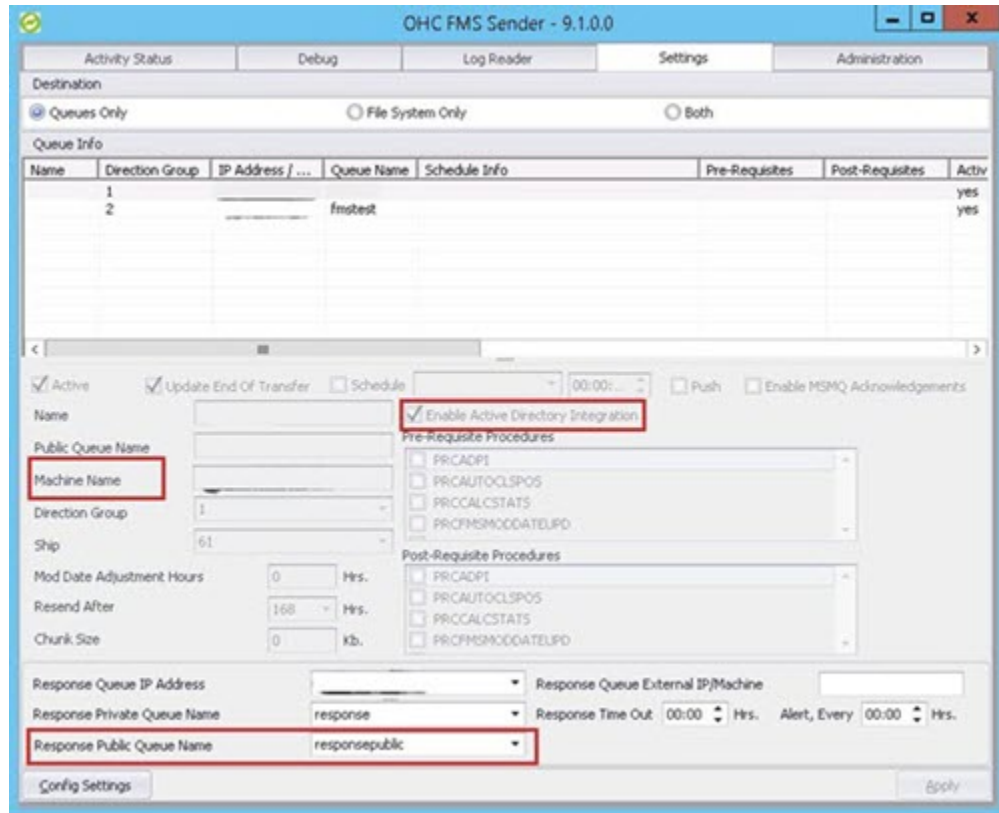
1. Login to your machine as a domain user, go to **Computer Management**, select **Services and Applications**
2. Expand Message Queuing, and right-click **Public Queues**.
3. Select **New, Public Queue**. The queue is to remain as non- transactional.

Figure 12-2 MSMQ Public Queue List

Creating Queue Settings in both Workgroup mode using private queues allow the domain user to run Sender/Receiver in both modes (Work Group and AD mode). The AD mode uses public queues to send or receive data. Also, an additional private response queue (Workgroup mode) and public response queue (AD mode) are configured to receive responses.

Sender Settings

Figure 12-3 Sender Settings Screen



1. **AD Mode:** Required to **Enable Active Directory Integration** and select **Response Public Queue name**.
2. **Workgroup Mode:** Select **Response Private Queue Name**.

Since the use of MSMQ is not limited to only Fleet Management, it is recommended to use intuitive queue names to reflect the locations they represent. For example, a fleet with three ships called MV Sun, MV Moon and MV Cloud, the queue names could be FMsun, FMmoon and FMcloud. However, to meet an operator's compliance guidelines, the names can be set as desired.

At the ship-side, when using two-way communications, the queue is expected to be utilized for administrative system messages. Oracle Cruise naming standard for this queue is FMdata, but like other shore-side queue names, this can be changed to meet a company's needs.

At queue creation, journaling must be enabled on all FMS MSMQ queues and validate that the queues were created as Non-transactional.

! Important:

See [Oracle Hospitality Compatibility Matrix](#) for compatible operating system and database clients..

When setting up the Interface Servers/PCs that runs the two components of the FM Transfer Interface, one must ensure that there is proper connectivity between the source and destination PCs. This can include troubleshooting routing and firewall.

Note:

While the Interface has been successfully tested on Windows 2000 and Windows 2003 platform, it is recommended to run the latest certified Windows OS, as each higher version of the OS supports a higher version of MSMQ which provides additional administrative functions for the Interface to manage the queue.

Interface Preparation and Best Practices

The item listed below is general practices for any Fleet Management System interface clients.

Turn Off Windows Updates

To ensure all day/every day uninterrupted processing of the Interface, ensure Windows Updates are turned off. Invoke Automatic Updates from the Control Panel to modify settings accordingly.

! Important:

The Customer must be informed, so that Technical Administration can be coordinated periodically.

Prerequisites

There are separate executables or installers for both the Sender and Receiver components. Both have its prerequisite for it to be installed and run. You must install the .NET Framework 4.6.1 or higher version before continuing to run the setup executables or installers as these are built upon its architecture.

Receiver

The Receiver is the second part of the FM Transfer Interface since it can act only if the Sender has sent any messages to its receiving queues. The Receiver continuously looks for messages within the queues defined in its Settings tab and processes them upon arrival. Like the Sender, the Receiver is a multi-threaded application that can process many messages simultaneously from many queues. Due to the administrative actions that need to be carried out on the receiving queues, the Receiver is limited to working with the queues on its OWN PC (or server). It can NOT work with queues that are setup on remote machines.

See [Configuring Sender](#) section for configuration steps and below table for configuration settings..

The settings are saved in an XML file called Config Settings. The password is saved in a 128 bit encrypted form. These settings can always be modified by clicking on the **Config Settings** button under the **Settings** tab of the FM Receiver.

 **Note:**

If any settings are modified or new queue entries are added, the Interface must be restarted for these settings to take effect.

Table 12-5 Config Settings

Configuration Setting	Description
Root Path	The Root Path is usually the folder where the executable resides. This is used by the Interface to create the sub-folders/directories where the Activity logs and Exception Log is written to.
File Retention Days	This number defines the days that the log files are retained. Logs greater than the number of days are purged.
Thread Pool Max Thread Count	The Receiver uses multi-threading technology to process many tables simultaneously at great speed. This number defines the count for the maximum threads that it opens at any given time. This number is usually derived based on the total tables to transfer + configuration of the PC running the Receiver + the configuration of the database servers since each thread makes its connection to the database. The Receiver divides the total threads by the total number of queues to process so all queues get equal resources and all are processed simultaneously.
Enable Tracking Service	This option allow you to choose whether to launch the Tracking Service to check if the Receiver is alive or not. If the Receiver is closed gracefully, the service writes an Informational message in the Application Event log and stops. If the Receiver is forcefully closed, the service writes a Critical Error in the Application Event log and stops. This Service can then be managed thru any Operational Management tool to send alerts as required.
Schema Info	In this grid, the database connection is defined. The TNS Names file must first be selected to enable the Interface to provide a list of all possible DB connections. This file typically resides in the NETWORK\ADMIN folder/directory under the Oracle Home folder/directory.

Fleet Management Receiver

The Fleet Management screen shows the following tabs:

Table 12-6 Tabs and their description

Tabs	Description
Activity Status	The Activity Status tab shows the current activity performed by the FMS Receiver. It also provides some other relevant information like the date and time of the last transfer and next transfer. The grid itself is self-explanatory and gives a running count and description of each message being processed.
Log Reader	The Log Reader tab enables retrieval of any old log file to see the details of the activity. A browser can be invoked to select the appropriate log file for viewing.

 **Note:**

A new log file is created for daily and is named accordingly. All logs are saved in XML format. Logs are retained in C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS Receiver\Queue-name\Log sub-folder/ directory for the respective queue.

 **Important:**

There are no automated procedures to purge log files. You must periodically perform clean-up contingent on disk-space availability.

Setting

The Settings tab is the place to set up all the queues that you want the Receiver to process.

Queue Info: This panel enables the user to provide the necessary information to define new queues.

 **Note:**

Be aware that a PC (or server) can have more than one IP address, additionally, if enabled, it could have IP version 6.

Table 12-6 (Cont.) Tabs and their description

Tabs	Description
Administration	<p>Time Blocking: This panel enables the user to add time-slots restricting the Receiver from processing any messages. This functionality is provided to accommodate customers' DB maintenance windows. The Receiver initiates the Stop Receiving command 5 minutes before the start of any time block.</p> <p>The Administration tab currently provides only 2 options; to stop or to start the Receiving process. When the Receiver application starts, the Receiving process starts by default. If for any reason, the Receiver needs to be put offline, just click Stop. The process will stop after processing all remaining messages in the memory. To start the receiving again, just click Start</p>

Adding Queue Info

1. Right-click into the grid and select **Add**.
2. Right-clicking on the specific queue enables the edit function, and brings the cursor to the lower half of the panel where you can select the correct IP address of the current machine.
3. Select a valid IP address. List of respective Private Queues are populated.
4. Select the correct queue and click **Apply**.

Syncing Data

From the shipside FM Sender's **Administration** tab, select **Transfer Management**, a specific date can be selected from which the synchronization starts. If a customer decides to retain all the available data from its first available backup, he/she can opt to use the options in Force Full Transfer instead. The drop-down of **Last Transferred Date** shows a calendar view on which you can scroll through the years and/or months. A date can then be selected.

1. Select a **Date** from the calendar view. If no specific tables are selected in the left-pane (not recommended during a historical database synchronization process), and a user click OK, the system will prompt for a confirmation.
2. If user click **Yes**, it will update the `Fidelio.FMS_Transfer.LAST_TRANSFERED` for all the tables.
3. Proceed to the **Manual Transfer**, and leave the default select-box **From Last Transferred**.
4. Click **Transfer** to commence the data transfer process, and the application reverts to the **Activity Status**.
5. The listed Status shows **Transfer in progress ...** immediately after Validating Transfer Table ..., and the data-synch commences.

As a high-level validation, Oracle Hospitality Cruise provides a summary script over some key data tables whose output can later be compared against the FM shore side database to ensure that all data has been transferred. Among the tables summarized are:

Tracking Record (Batch Level)

The batch level tracking records is a feature of Sender and Receiver. This section explains the tracking process and how to configure the tracking record.

Record Level Tracking Process

For records level tracking, the columns in FIDELIO and FCONSOL Schema are as follows:

- SUCCESS_ROWS >> FMS_TRAN_LOG
- STATUS >> FMS_TRANS_AUDIT
- ERROR>>FMS_TRANS_AUDIT
- REMARKS>>FMS_TRANS_AUDIT

Status column is marked as required, and the initial status is 0. The receiving side status become 7 or 8 (depending upon success or error) and the same is applied to the sending side. Sending side, retain records whose status is <> 7 for resending.

The record level tracking process is as follow:

1. **Sending Side:** ACC >> Records in a Batch ID for example are 10 records with the status initial as 0 in the `fms_trans_audit` table. Each record in `trans_log` with the same `batch_id` will be inserted for batch level information and send it to the Receiver on the Receiving Side.
2. **Receiving Side:** Receiver processes the `batch_id` and inserts 10 records in the `fms_trans_audit` table. For example, if 2 records are `Error` and 8 records are `Success`. The Receiving Side will send the same status to the Sender as a Response message.
3. **Sending Side:** The Sender processes the response message and marks the status in the `fms_trans_audit` on the Sending Side. Each of success record is marked as 7 and it will be deleted. For each of error record is marked as 8 and the Sender will resend the failed records until they are fixed.



Note:

Some errors may require the help from a support team or from a Database Administrator (DBA) consultant. For example:

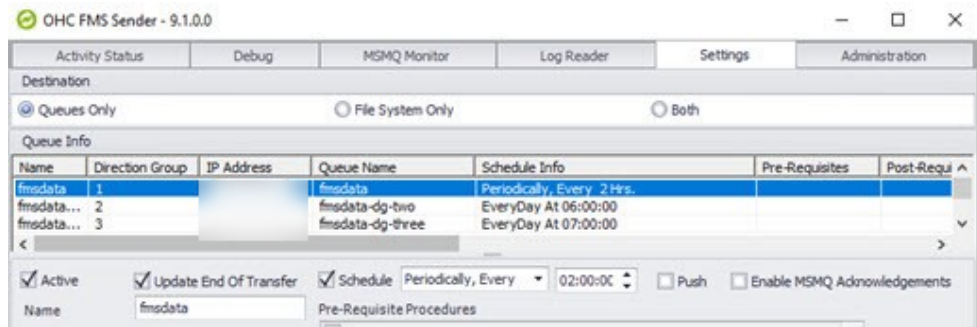
- When you are trying to add data for a mandatory column but the column is missing from the database table.
- The FMS Transfer entries are incorrect.

Tracking Records Setting Steps

The batch level tracking of records is a new feature of Sender and Receiver. Batch level tracking is explained in the following steps.

1. Data transfer of tables occurs through batches.

Figure 12-4 Direction Group Queue Must Be Active and Schedule Must Be Checked



- In the Sender interface, the direction group queue must be active and the schedule must be enabled.

Figure 12-5 FMS_TRANS_LOG in FIDELIO Schema

TABLE_NAME	TRANSFERRED_DATE	BATCH	SOURCE_ROWCOUNT	TARGET_ROWCOUNT	SOURCE_REMARKS	TARGET_REMARKS	FMS_TRANS_LOG_MODDATE	STATUS	SOURCE_ASSET_COUNT	TARGET_APPROXIMATED_COUNT	BATCH_ID
3 CDR	17-SEP-2019 05:29:19	1/3	96	96	Skipped 6 Row(s)		17-SEP-2019 05:29:22	8			1 942000000183446
2 CDR	17-SEP-2019 05:29:17	2/3	111	92	Skipped 19 Row(s)		17-SEP-2019 05:29:20	8			1 942000000183447
3 CDR	17-SEP-2019 05:29:16	3/3	21	21	(null)	(null)	17-SEP-2019 04:18:59	7			6 942000000183448

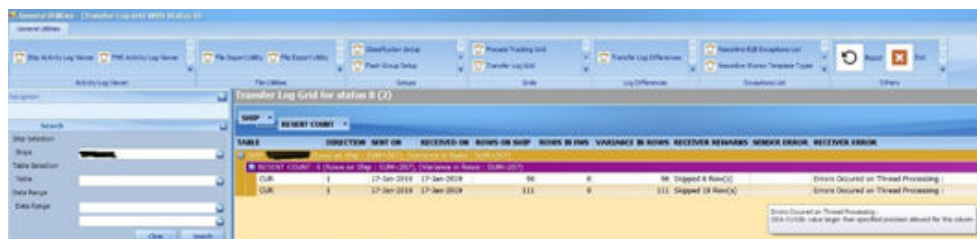
- The FIDELIO.FMS_TRANS_LOG and FCONSOL.FMS_TRANS_LOG table contains the transferred records information.

Figure 12-6 FMS_TRANS_LOG in FCONSOL Schema

TABLE_NAME	BATCH_ID	TRANSFERRED_DATE	RECEIVED_DATE	BATCH	SOURCE_ROWCOUNT	TARGET_ROWCOUNT	SOURCE_REMARKS	TARGET_REMARKS	FMS_TRANS_LOG_MOD...	STATUS
1 CDR	\$420000000183447	17-SEP-2019 04:...	17-SEP-201...	2/3	111	0 (null)		Skipped 19 Row(s)	17-SEP-2019 05:29:24	8
2 CDR	\$420000000183446	17-SEP-2019 04:...	17-SEP-201...	1/3	96	0 (null)		Skipped 6 Row(s)	17-SEP-2019 05:29:20	8
3 CDR	\$420000000183448	17-SEP-2019 04:...	17-SEP-201...	3/3	21	21 (null)	(null)		17-SEP-2019 04:18:58	7

- The **Status** column in **FMS_TRANS_LOG** table signifies the following:
 - status=7** signifies the table has been transferred successfully.
 - status=8** signifies the table transferred has been failed.
- The Batch ID of the records with **status=7** in **FMS_TRANS_AUDIT** table are the records which transferred successfully and **status=8** are the records with errors in FCONSOL schema.

Figure 12-7 Transfer Log Grid With Status 8



- In the FMS Desktop application you can view batch level transfer error log on **Transfer Log Grid With Status 8** screen and **Transfer Audit Grid** for viewing the record level error.

Figure 12-8 Transfer Audit Grid

BATCH ID	TABLE ID	BATCH	NEXT DT	NEXT TIME	REJECTED DT	REJECTED TIME	STATUS
SCH0000000000	SCH00000000	01	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	02	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	03	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	04	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	05	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	06	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	07	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	08	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	09	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	10	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	11	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	12	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	13	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	14	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	15	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	16	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	17	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	18	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	19	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped
SCH0000000000	SCH00000000	20	17-Jan-2019	09:03:26	17-Jan-2019	09:26:39	ORA-01438: value larger than specified precision allowed - Stopped

13

Corporate Access Module

Oracle Hospitality Cruise Corporate Access Module (CAM) is a solution that helps you to manage and govern the visitor's corporate access to various departments including ships.

Figure 13-1 Corporate Access Module Architecture

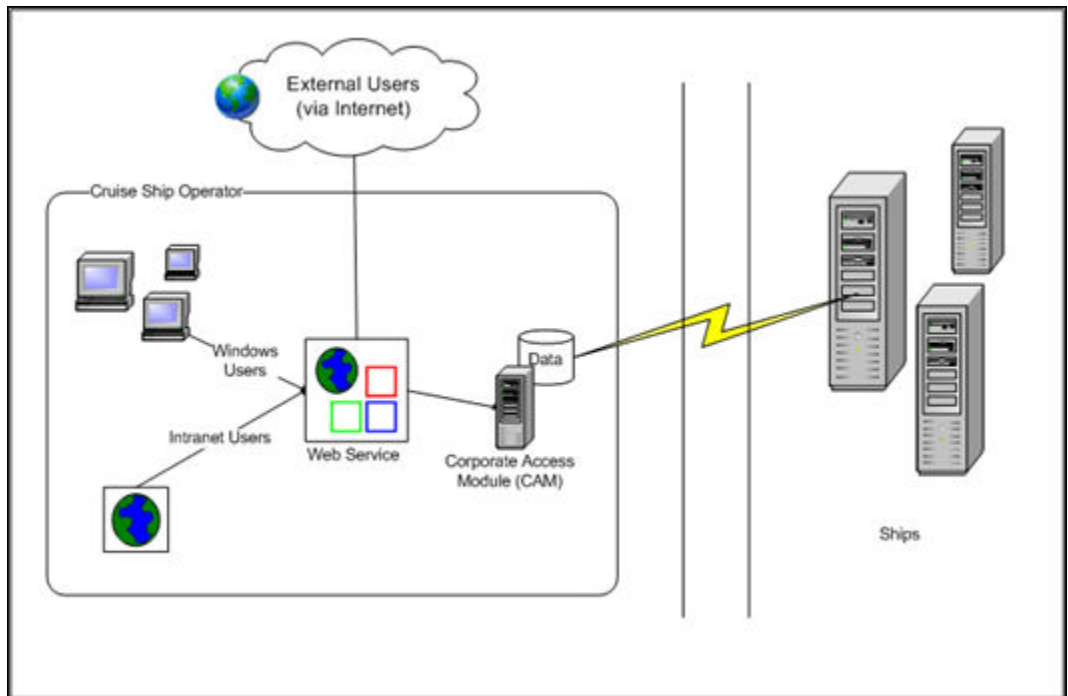
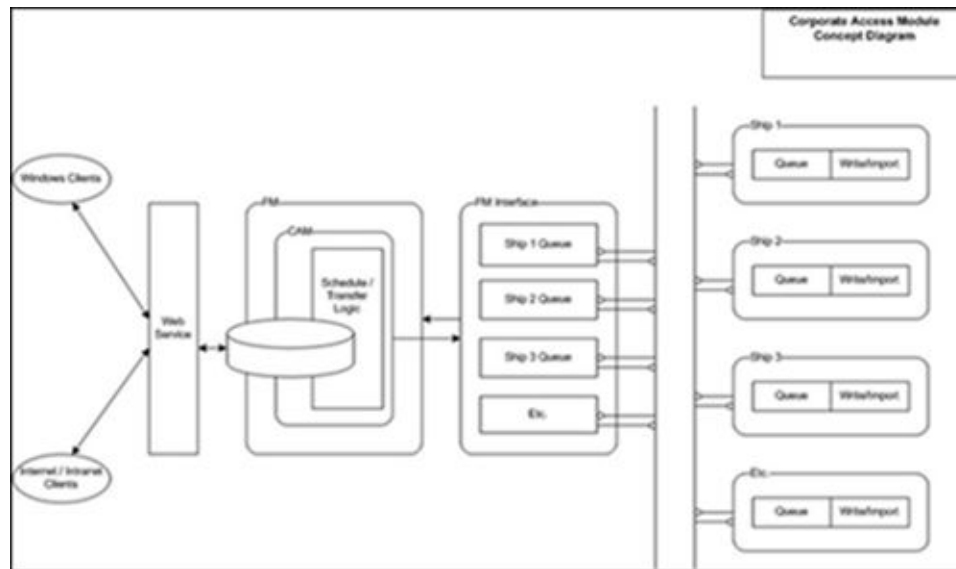


Figure 13-2 Corporate Access Module Data Flow



Business Flow

Visitor Creation

Visitor's details can be created by adding the mandatory details with live picture taken or uploaded, passport and other important documents can be scanned and saved.

Visit Creation

Visit details for a particular visitor are added into the system by mentioning the location and date for the visit along with the reason for the request.

Approval Request

Approvals requests can be sent via email to the concerned person. There is also a provision of sending requests or rejecting a request from the system, along with the reason.

Visit Approval

A group of approvers predefined in the system can Approve/Decline the visit via email or through the system. All email functionality can be configured within CAM. The approvals can also be sent via web approval system.

Data Transfer

Sending and receiving of data can be done through two separate modules called FMS Sender and Receiver.

- Sending data - The Sender executable runs on a shore side machine, transfers data to the ship (using MSMQ), and receives conformation messages from the ship once the message is received.
- Receiving data - The ship side receives the data and inserts them into the SPMS DB. The receiver sends response to the sender.

Visitors

The Visitor tab has six modules:

- Visit Overview
- Visitors
- Approvals
- My Requests
- Crew Family Details
- Orphaned Emails

Visit Overview Form

Visit Overview gives a list of visits planned for various locations based on the date range selected in the calendar. When you select a date range from the calendar, all visits within this time duration appears on the lower grid indicating the visit locations and the number of people visiting in a day, with the number of people who have their visits approved and those that are pending. On the left side of the screen, the visit locations are listed showing the number of maximum people permitted on each day.

The selection of visit locations on upper right can be changed to display the data according to the specified location on the calendar view. Double clicking on any visit detail cell opens the visitor's details including visits for editing. You can added new visitor or a visit request from the screen, or edit the visitor's data. All the tabs of the screen are explained later in the document. You can also search for a visitor from the lower left column, and dragged and dropped to the record of another visitor on the upper left column if there is a need to assign same visit date to that visitor.

Table 13-1 Visitor details fields

Visitor Details	Description
Last Name	Last name of the visitor.
First Name	First name of the visitor.
Salutation	Pre-fix assigned to the name.
Passport/ID No	Passport or ID Number of the Visitor.
Visitor Type	Type of the visitor.
Validity From	The document is valid from this date.
Validity To	The document is valid till this date.
Date of Birth	Birthdate of the visitor.
Email Address	Email address of the visitor.
System Account	System account of the visitor.
Authorization Code	Authorization Code of the visitor.
Remarks	Remarks mentioned about the visit/visitor.
Upload Picture	Use to upload visitor image

Visitors Form

Select the visitors' icon. Visitors form is the second form in the application and here all the visitors can be viewed at a glance. The grid shows existing visitors and highlighting any row will give you the details including picture at the bottom left section. On the bottom right, there is a grid showing list of all visits for that person. The historical visits of a person can be viewed along with upcoming visits. A new visitor can be added by clicking the **New** button in the menu bar.

Adding a New Visitor

Personal details of the visitor can be entered on this screen. This includes the first name, last name, salutation, and the passport number. Picture of the visitor can be taken and stored here itself by clicking **Start camera** and when the visitor is ready, press the **Take Picture** button. You can also upload the picture by pressing the **Upload Picture** in the middle section. The picture can be cropped accordingly before uploading it. Passport of the visitor can be scanned by putting the passport on the scanner and clicking **Read Passport** button. All the personal details including picture of visitor would be read by the scanner and reflected on screen to save.

To add,

- Click the **Visitors** tab and select **Search**
- The Search panel can be pinned to the screen by clicking on **Pin** button at the upper right of the panel.
- The Search panel of the Visitor Maintenance screen gives the option to search visitors based on personal information like name, date of birth, passport number, etc
- Visitors can be searched from visit related details, time period of visit date and visitor validity
- Visitor can be assigned the same date which is assigned to another visitor by searching the visitor in the lower left corner of the screen and when the search is over dragging and dropping the visitor record to the upper left of the screen.

Editing Visitor's Record

A record can be edited by double-clicking a visitor's data from the grid.

A visitor is enabled by default and you can disabled using the **Disable Visitor** button. All required privileges can be edited or granted to each visitor by selecting the privilege column on the right. Any document relevant to the user can be added and their information would be stored in the second tab of the user details sections. Press the **Scan ID** button to scan and store the documents of that visitor. The MRZ fields (MRZ1, MRZ2, MRZ3) is machine readable zone code scanned by the system when it is configured with a scan card reader.

Approvals

To view a list of approvals, click the **Approval** icon. The list contains the login IDs and this can be checked against their approval or rejected status. Use the **Approve/Reject** option to approve or reject the visit.

The Search panel lets you search by request status, visit location as well as other personal details of the visitor. Visits can also be approved or rejected by selecting the visits and pressing the CTRL key, and selecting the **Approve/Reject** option.

My Request Form

My Request summarizes all visit requests created by a user and enables them to know the status of the request created. To access, select the **My Request** icon from the menu bar. To view the approval/rejected status of the visit, search the Visitor Information. You can search based on status, visitor category, visitor type, visit location, request status, pending with (the person or the group which has not submitted the approvals in a specified timeline), as well as the start and end date.

Crew Family Details Form

The Crew Family Details form lists the crew members and provides the search option based on the details of crew member, the visitor information of the visitor, and on other criteria.

To link visitor to the crew:

1. Select the **Visitors** tab, and then click the **Visitors** icon.
2. Double-click the visitor row to select a visitor.
3. On the **Visitor Details** tab, select a **Visitor Type**.
4. Click the **Crew** link adjacent to the **Visitor Type** drop-down button.
5. Search for the crew name which the visitor details would be linked. Double-click the crew name to select it. The visitor is now linked to the crew. The crew member name is displayed on the visitor details form.
6. Click **Save**.

Orphaned Emails Form

Emails that are not associated with a visit are listed as orphaned emails. Search a visit by the visitor name or by other fields on the left column. Select an email from the **Orphaned** email section associated with the visitor, and then drag it to the **Visits** section. To process or discard an orphaned email, drag and drop it to the **Process** button to process it or **Discard** button to discard

Crystal Reports

Crystal reports can be added to print details about the data in the CAM system. CAM groups reports based on:

- CAM Reports - All reports having visitor/visit details.
- WKF Reports - All reports having email related data.
- Admin Reports - All setup level reports.

Setup

This option is only available for the thick client. The web application status configuration along with the hardware setup can be set from this section.

System Parameters

System parameters are divided into Consolidation, General, Login parameters and messaging parameters. The system required parameters can be set up here.

Business Entities

Location profile can be made from business entity section. A business entity is used to provide important information to the system like the location where the visitor would go - ship or building.

Table 13-2 Business Entities

Business Entities	Description
Company Name	The name of the company arranging the visit.
Company Type	The location, whether it is ship or building.
Code	Code of the location.
Name	Name of the location.
Remarks	Remarks given to the location.
Maximum visitors for this location	Maximum numbers of visitors for the location.

Table 13-3 Number of override visitor with permission

Field	Description
Approval cutoff period	Number of days before the actual visit.
Generic card sequence	Generic card sequence number from start to end.
Building Address	Address of the building.
Building Timings	Timings of the building for which the visit would be assigned.
Require Prior Approval	Check this button to assign the approval group.
Default Approval group	Once the default approval group is assigned for a particular building, the system would automatically take those approval group as default approval groups, and you need not assign approval group again for that building.
Active	Check Active when the location needs to be shown in the system otherwise uncheck it in order to hide it.

Visitor Categories

Visitor categories are divided into two subsections:

- Visitor Type
- Approval Assignment

Visitor Type. Visitor Type consists of the following fields:

Table 13-4 Visitor Type Fields

Fields	Description
Name	Name of the Crew Type.
System Account	The system account can be selected from the drop-down menu bar.
Category	Select the category of the crew from the drop-down menu.
Priority	Priority of the crew in comparison with another crew types.
Approval Required	Select approval if required and no approval if the approval is not required.
Require Letter	If a letter is required then click the check box button.
Allow Early Boarding	If early boarding is required then click enables early boarding check box button or else leave it unchecked.
Permanent Visitor	If the crew is a permanent visitor then click it.
Visitor Board Card Report Template	Select the visitor board card report template according to the crew visitor.
Privileges	Privileges assigned to the crew.
Crew Type	If this is checked, link the crew type before enabling the visitor type.

Click **Save** at the options bar to save the changes.

Approval Assignment

Approval Assignment tab allow you to set up the Approval group for a visitor type, and enables assignment of approval hierarchies. The threshold period is a time period assigned for submission of approval or rejection of visit status. The email is first sent to Selection 1 within a group and the limited time period is assigned for the status. For example, for approval or rejection by the person. The threshold is the approval time period given in days and hours.. After the threshold period for Selection 1 expires, the email is sent to the Selection 2 within the group. This process is repeated till all the selections and the groups have been covered.

If all the selection in the 1st group approves a visit then only the email would go to the selections of the 2nd group. Otherwise the email would not be sent to the second group. If there are two group levels, group 1 approves a visit and group 2 also approve a visit then only the visit is approved. In the same scenario, if the group 1 approves a visit and group 2 rejects a visit then the visit would be in conflict.

Visitor Privileges

The privileges assigned to the visitor can be defined here with code and comment regarding the privileges. On the column on the right, visitor privileges can be added by selecting the check-box button.

Approval Groups

The privileges would be assigned to a particular approval group. You can only select one approval group at a time from the drop-down menu. To select the user privileges that should

be given to a particular group, click the check box button. Multiple privileges can also be selected for an approval group. Approval groups can be setup in FM and assigned to a group. All approval groups setup in FM come under unassigned.

Document Setup

Document setup is used for setting up corporate management related documents as a prerequisite for a visit. Select the **Category**, click the file path logo adjacent to the file path after the input box. The system would prompt for assigning the path for the document file. The document can be uploaded into the system by clicking the **Upload** button. The file name and file path appears after you click the **Open** button.

Hardware Setup

You can configure scanners such as DeskoPenta for use in Corporate Access Module so that the visitor information can be scanned and entered into the system. You could also configure the Web cam for images/picture and Evolis Primacy printer to print the cards.

General

The information regarding the CAM system can be accessed from the General tab. The General tab contains three subsections:

- Utilities
- Skins
- Settings

Utilities

The General tab contains the File Import and Export utility. Using a template, file can be imported or exported.

- **File Import Utility**- Select the **File Import Utility** to import a file. Click the **Load** button below the template input box.
- **File Export Utility**- You can export the document file on the system with this function. The data related to the file would be displayed on the screen.

Skins

Skins are used to change the look and feel of the Corporate Access Module. Select a color and then save the settings. On the next login, the new skin is saved for the user.

Settings

User is setup in FM for CAM at the time of first login. The user is prompted to fill in an email id, which is mandatory for CAM users and approvers.

14

Report Auto Sequencer

Oracle Hospitality Cruise Report Auto Sequencer is used to send the scheduled reports automatically. Today's schedules provide the information about the today's schedules status.

Table 14-1 Today's schedules

Schedules	Description
Emails Pending	Shows the emails that are yet to be sent
Schedules Done	Shows the number of schedules that are completed
Schedule Failed	Shows the number of schedules that are failed
Total Today's Schedules	Shows the total number of schedules which are scheduled for current day
Next Schedule Time	Shows the time of next schedule
Next Transfer In	Shows the time left in next schedule

Schedule Details

1. To edit already existing schedule, right-click the left vertical panel and select **Edit**
2. On the right side, enter the email addresses of the recipients in the distribution list
3. Check the status of transfer as **Active**. Output type should be provided along with the report schedule settings
4. Click **OK** to save the settings

Settings

1. To add a schedule, right-click the left vertical panel and select **Add**
2. On the right side, enter the email addresses of the recipients in the distribution list
3. Check the status of transfer as **Active**. Output type should be provided along with the report schedule settings
4. Click **OK** to save the settings

15

Encryption Manager (EM)

The purpose of Encryption Manager (EM) is to provide guidelines to change the encryption key within Fleet Management.

The Encryption Manager screen has the following tabs:

Table 15-1 FMS Encryption Manager Screen

Tabs	Description
Encryption	<p>This function allow you to select and decide the column(s) to encrypt.</p> <p>You can view the currently decrypted columns and add columns as part of an encryption.</p>
Decryption	<p>Tab shows the columns that are encrypted and need to be removed from encryption, and information are shown as plain text in future. You can select and decide whether to decrypt it from the currently available columns.</p>
Encryption Key	<p>This tab is used to rotate the key. It auto decrypts the encrypted data with the original key in AES-CBC mode, update the new key, and encrypts data with a new key in AES-GCM mode. AES-GCM mode will not enforce immediately the migration of data upon upgrade. It uses the previous AES-CBC mode. This will only take place when you choose to rotate the key..</p>
Encrypted Data PCI Adjustment	<p>Function retrieves the data that is older than a year and in an encrypted form, decrypt it and masks the number except last 4 digits >, and then re-encrypt before storing the data.</p> <p>Example:</p> <ul style="list-style-type: none">• PLAIN: 1233456789081114• ENCRYPTION: AXS12556HSndhdhsdjhwd781738• DECRYPT: 1233456789081114 if the credit card is older than 1 year then MASK. MASK-XXXXXXXXXXXX1114• Re- Encrypt: AXS12556HSndhdhsdwewvh232vvevevr38• Decrypt: Only last 4 digits are available on the screen

Table 15-1 (Cont.) FMS Encryption Manager Screen

Tabs	Description
Conversion from Old to New	<p>This function retrieves the encrypted data and decrypt it using the old method and encrypt it with the new method.</p> <p>FMS Encryption Manager fetches the information from the Encryption table and knows whether the data is in FMS or SPMS method.</p> <p>If the FMS Sender (FM sender 8.4. and above) uses the old method, you need to first install the Encryption Manager and convert the data to new method using this tab.</p> <p>The latest version of Sender uses only the SPMS new algorithm and does not support the old method.</p> <p>There is a prerequisite to run the script <code>FMS_FCONSOL_ALTERS.SQL</code>.</p> <p>When converting from old to new method, it checks for all data that has NULL in the Encryption Type column, convert and is marked it as new.</p> <p>Prerequisite: Select FidelioBK in Sender and Receiver on both sides.</p> <p>The scenarios can be:</p> <ul style="list-style-type: none"> • Data is stored in FMS encryption method • Data is stored in SPMS encryption method but using Old key • Data is stored in SPMS encryption method but using New key <p>Old method = FMS or SPMS (old algorithm). New method= SPMS (new algorithm). SPMS 8.0 and above uses the new algorithm explicitly. FMS Data Viewer also must be v8.4 and above.</p>
RSA Encryption Key	<p>Third-party vendor/reservation system encrypts the reservation files with the Public Key generated by Encryption Manager before sending the files to Microsoft Message Queuing (MSMQ). The Private Key stored in the CDTI XML Template is used to decrypt the incoming files in MSMQ before inserting them into the Corporate Data Transfer Interface (CDTI).</p>
PGP Keys	<p>Function in this tab uploads the PGP public key of the ship to the database with AES encryption. This public key is used by FMS ResOnline to encrypted the reservations credit card PAN in FCRESVINT, allowing DGS ResOnline to decrypt it with the ship's private key.</p>
Settings	Use to view and configure settings.

To process credit card data, you must first upload the Public Key using the FMS Encryption Manager for Reservation Online to encrypt the credit card number when processing the data. You need to upload the PGP Key pair to both FMS and SPMS so that SPMS can decrypt the credit card number received from FMS.

Before you upload or change the PGP Key on both FMS and SPMS, you must:

1. Ensure that there are no pending transactions in Reservation Online (FMS) and DGS Resonline (SPMS).
2. Generate new PGP Key pair using a third-party application.
3. In SPMS, upload the new PGP Public and Secret (Private) keys with OHC Tools, DGS Credit Card Set 1 or DGS Credit Card Set 2 tab.
4. Provide the new Public Key to FMS (Shore side) and third-party reservation system.
5. Update the new Public Key in FMS using Encryption Manager, PGP Key function.
6. Restart the FMS Reservation Online to apply the new key.

Changing FMS Encryption Key

Prerequisites

Prepare a new encryption key with 8 — 16 digits. This key can be generated using an external key generator software.

Before You Begin

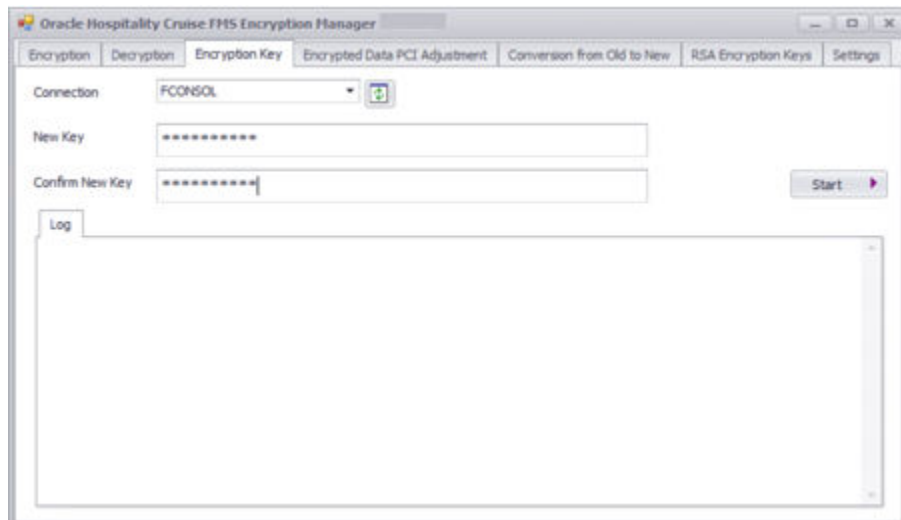
The below tasks are **Mandatory**. You must ensure the criteria are met to avoid any adverse impact on the system.

1. OHC Sender/Receiver (Shoreside) is **not** running.
2. Exit **OHC WatchDog**. If you did not exit the OHC WatchDog, it will restart OHC Sender/Receiver.
3. Close all FMS applications. All read/write access to FMS DB is not allowed.

Steps to Change the FMS Encryption Key

1. Run **FMS OHC Encryption Manager**.
2. Select the **Encryption Key** tab.
3. Select a schema from the **Connection** drop-down list.
4. Enter the new key.
5. Click the **Start** button.

Figure 15-1 FMS Encryption Manager



Completing the Key Rotation

1. Restart the FMS shore Sender/Receiver.
2. Run FMS application and verify if PII data is viewable.

Emergency Response System (ERS)

The Emergency Response System helps in controlling and managing the passengers, crew, and visitors during an emergency onboard the ship, by identifying the latest onboard status and can be use to update their emergency contact information.

Logging in to Emergency Response System

The first screen of the Emergency Response System web application is the login screen, which would require your Fleet Management credentials to log in.

1. In the upper left of the drop-down list, select the language of your choice.
2. Enter your **User Name** and **Password** to access the information about the ship, or click **Family member's Login** to directly access the information about your family members. **Family Member's Information** screen is displayed.

You can access the family member's information for crew and passengers from here.

3. On the **Family Member's Information** screen, select the **Passenger** check box to find the information for passengers family members and **Crew** check box to find the information for crews family members.

All fields are mandatory.

Activating Emergency Record Transfer

In case of emergency, the first step required is to add Passengers, Crew and Visitors information to ERS

1. Login to OHC FMS (Data Viewer)
2. Ensure your ERS user name is a member of ERS or Administrator Group
3. Click **Reporting and Utilities**
4. Click **General Utilities**
5. Click **Ship Setup**
6. Right click the ship in emergency and click **Edit**
7. Click Show on **ERS** and **OK**

! Important:

On enabling "**Show on ERS**" flag, this enabled the frequent data transfer from ship to shore. This flag should **ONLY** be set in case of emergency

Viewing Vessels in Emergency

If there is any vessel in an emergency, you can view it. The vessel in an emergency shows the Passengers, Crew and Visitors information.

1. Click **Vessel Emergency**, and the **Vessel Emergency** screen appears.
2. The **Vessel Emergency** screen shows the name of the vessel, information of the passengers, crew and visitors of that vessel. It also shows the number of passengers needing assistance under **Need Assistance**.

The grid includes the following passenger information:

Table 16-1 Vessel Emergency Information

Information Displayed	Description
Checked In	Number of checked-in passengers, crew, visitors, and those that need assistance.
Onboard	Number of onboard passengers, crew, visitors, and those that need assistance.
Shoreside	Number of at shore side passengers, crew, visitors, and those that need assistance.
Missing	Number of missing passengers, crew, visitors, and those that need assistance.
Verified	Number of verified passengers, crew, visitors, and those that need assistance.
Not Verified	Number of non-verified passengers, crew, visitors, and those that need assistance.

3. Click the numbers under **Passengers, Crew, Visitors**, and **Needs Assistance** passengers to know the details about the passengers in distress.
4. Clicking on the numbers will open another window, showing the number of passengers and information of each status.
5. Repeat the above for **Onboard** and **Shoreside** passengers.

Viewing Passenger Details

1. Click the name of the passenger to view the passenger details. The Passenger Details screen appears.
2. Enter **Person Details** in the given fields.
3. Enter **Emergency Contact Details** in the given fields.
4. Enter **Travel Agent Details** in the given fields.
5. Enter the following **Additional Details** in the given fields.
 - **Life Boat:** Location of the life boat on the ship.
 - **Muster Station:** An area where all passenger gather at the time of performing mock drill/announcement from the captain.

6. On **Passenger Details** screen, click **Emergency Information**. Enter the emergency information in the given fields.
7. On **Passenger Details** screen, click **View Change Log**. Log is maintained by the Emergency Response System web application and it is displayed on the **View Change Log** screen.
8. On **Passenger Details** screen, click **Travelling With**. This screen shows the data of the people who are traveling with passenger.

Gangway Activity

Gangway Activity tracks the movement of visitor/passengers/crew at the gangway.

Viewing Gangway Activity

1. Log on to the Gangway Activity application to search for the relevant data of the gangway movement of visitor/passengers/crew.
 - a. Enter the username and password.
 - b. Select the Language of your choice from the drop down list.
 - c. If you enter the wrong credential, an error message is displayed, and you are not able to log in.

 **Note:**

FMS credentials can be used to login Gangway Application.

- d. On the Gangway Application screen, it shows the details of the logged in user's name and other information about the application. The list shows User Profile, Help, About, and Sign Out options.
- e. On selecting the User Profile, a popup appears and shows all the groups associated to the logged in user.
2. Click **Search**. Enter information in all the required fields to perform a detailed search. The search results are displayed in the right pane.
 - a. On the left of the search menu, you can search with the basic search criteria such as selection of Ship, Voyage, and Passenger's name.
 - b. Click **Show Advance Search** for more search features, such as Booking number, Gender and Activity date of user.
3. Based on the user search criteria, the result appears on the right side of the Search panel screen. The search results for that particular passenger is displayed.
 - a. On the Gangway Application screen, the **Search Menu** is for hiding and showing side bar and the **Report** button is to download the report result in PDF format. You can view image in different sizes, small, medium and large.
 - b. Use the **Go** button to type a column name or drag and drop a column from the table. The result shown are according to the selected Groups.

Table 17-1 Search Details

Details	Description
Person Details	Details of the Passenger/Crew/Visitor.
Image	Image of the Passenger/Crew/Visitor.

Table 17-1 (Cont.) Search Details

Details	Description
Ship	Ship Name of the Passenger/Crew/Visitor.
Voyage	Voyage Name of the Passenger/Crew/Visitor.
Name	Name of the Passenger/Crew/Visitor.
Cabin	Cabin number Passenger/Crew/Visitor.
Type	Type of the user ex: Crew.
Age	Age of the Passenger/Crew/Visitor.

Some additional columns are also added when performing the advance search selection. For example, Gender, Activity Date, and Booking Number, when the specific is selected. Columns can be reordered by selecting any column and drag and drop to the preferred position. Sorting is also allowed in the table data. Filter results are based on the selected value.

4. Click the **Filter** icon on the table column header to select filter value.
To remove any filter, you can remove the selected data for filtering. Group the result on various columns. It is also possible by dragging and dropping columns directly from the table.
5. Click **Enter** or **Go** to see data in groups. When you click every Passenger entry, you can see the details of that passenger in a popup window. This page also provides Report generation.
 - a. Click the Cabin number to view the number of occupants in the cabin. Other details such as **Voyage, Name, Type, Age**, and **Gender** are also shown.
You can view other users associated with the same cabin by clicking the cabin number in Passenger Information popup window.
 - b. Gangway application provides two reports. One is with the Passenger list in main search page and second is for Passenger's specific data in Gangways User Information Popup window. First page downloads report for all the Passenger/crew and visitors named UserListReport.pdf.