Oracle® Hospitality Cruise Shipboard Property Management System

Mobile Mustering and Gangway Security Installation Guide

Release 20.2
F44446-04
December 2023

ORACLE

Oracle Hospitality Cruise Shipboard Property Management System Mobile Mustering and Gangway Security Installation Guide, Release 20.2

F44446-04

Contents

Preface

The Mobile Mustering and Gangway Security is an add-on module to Oracle Hospitality Cruise Shipboard Property Management System (SPMS) that runs on a Microsoft Windows 10 IoT platform. Its core purpose is to process passenger and crew embarkation and administer movement on the Gangway using a Microsoft Windows 10 Mobile /Tablet. This document describes the full setup of the Mobile Application Server, OHC Webservices and Mobile Gangway client on mobile devices.

Audience

This document is intended for project managers, application specialists, and users of Oracle Hospitality Cruise Shipboard Property Management System.

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screenshots of each step you take

Documentation

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

Revision History

Table 1 Revision History

Date	Description of Change
September 2021	Initial publication.

Table 1 (Cont.) Revision History

Date	Description of Change
January 2022	Revised the usage/steps on following topics: • Adding Roles to Microsoft Windows Server 2012 R2. • Verifying the SSL Connection. • OHCruise Web Services. • MobileSync Interface. Removed the following outdated topics: • Generate IIS Self-Sign Certificate. • Binding the Self-Sign Certificate. • Connecting Mobile Devices to PC. • Turn on device discovery and pairing. • Connecting to Device Portal. Windows Device Portal.
July 2022	Made minor grammatical changes.
December 2023	Updated new customer portal.

Prerequisites, Supported Systems, and Compatibility

This section describes the minimum requirements for the Application Server for the Mobile Mustering and Gangway Security module.

Prerequisites

- FCMobile Database.
- Patch 33492113: OHC Shipboard Property Management System Mobile 8.0.6.
- Cabin Station Setup.
- Application Server for Mobile Services.
- Preinstalled Oracle Data Access Components (ODAC) for PC running SPMS applications.

  ODTwithODAC112030 or
  ODTwithODAC121021

Supported Operating System

- See Compatibility Matrix at http://docs.oracle.com/en/industries/hospitality/.

Supported Hardware

- Oracle MICROS 721 Tablet.
- Windows Mobile device with a camera.
- Server based CPU (Xeon X3440 2.53 GHz).
- Minimum RAM 8GB.

Compatibility

SPMS version 20.2 or later. For customers operating on version 20.2 and below, database upgrade to the recommended or latest version is required.

1

System Schematic

The Gangway Security and Mobile Mustering application consists of several components, and these components are responsible for transmitting information between the mobile device and the SPMS database. The following diagrams further illustrate the schematic flow between the components.

Figure 1-1 Gangway Security System Schematic

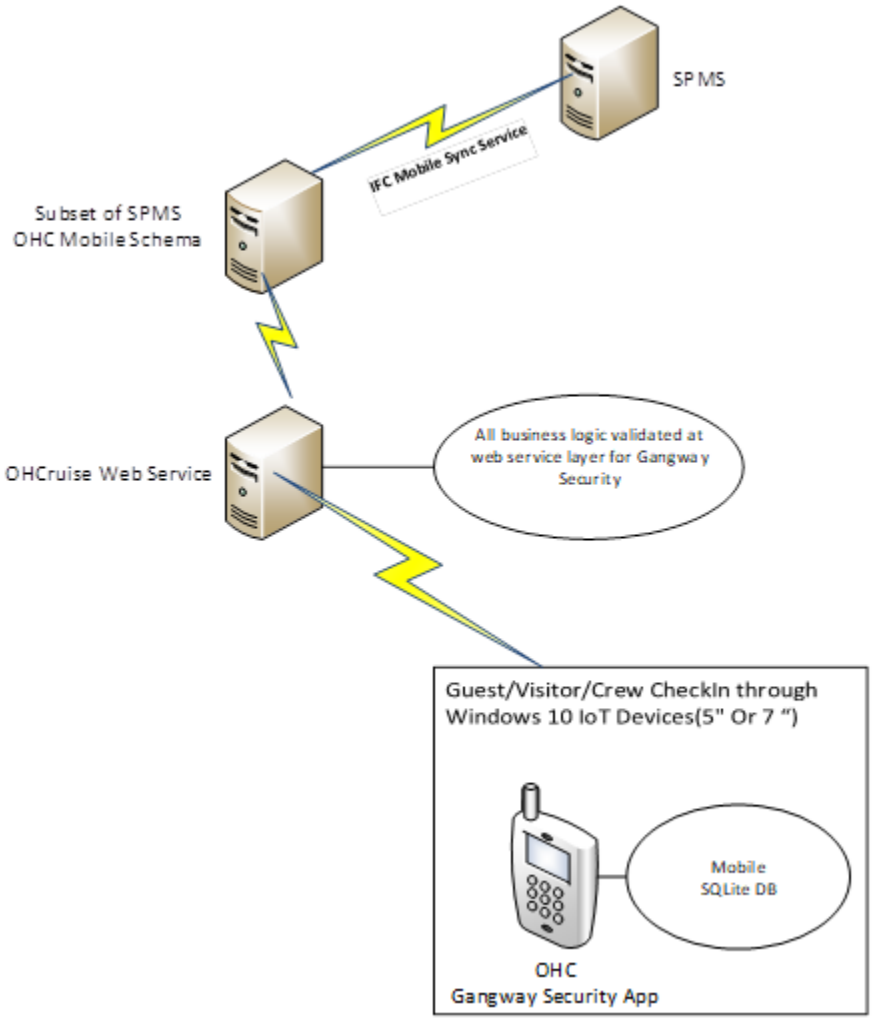
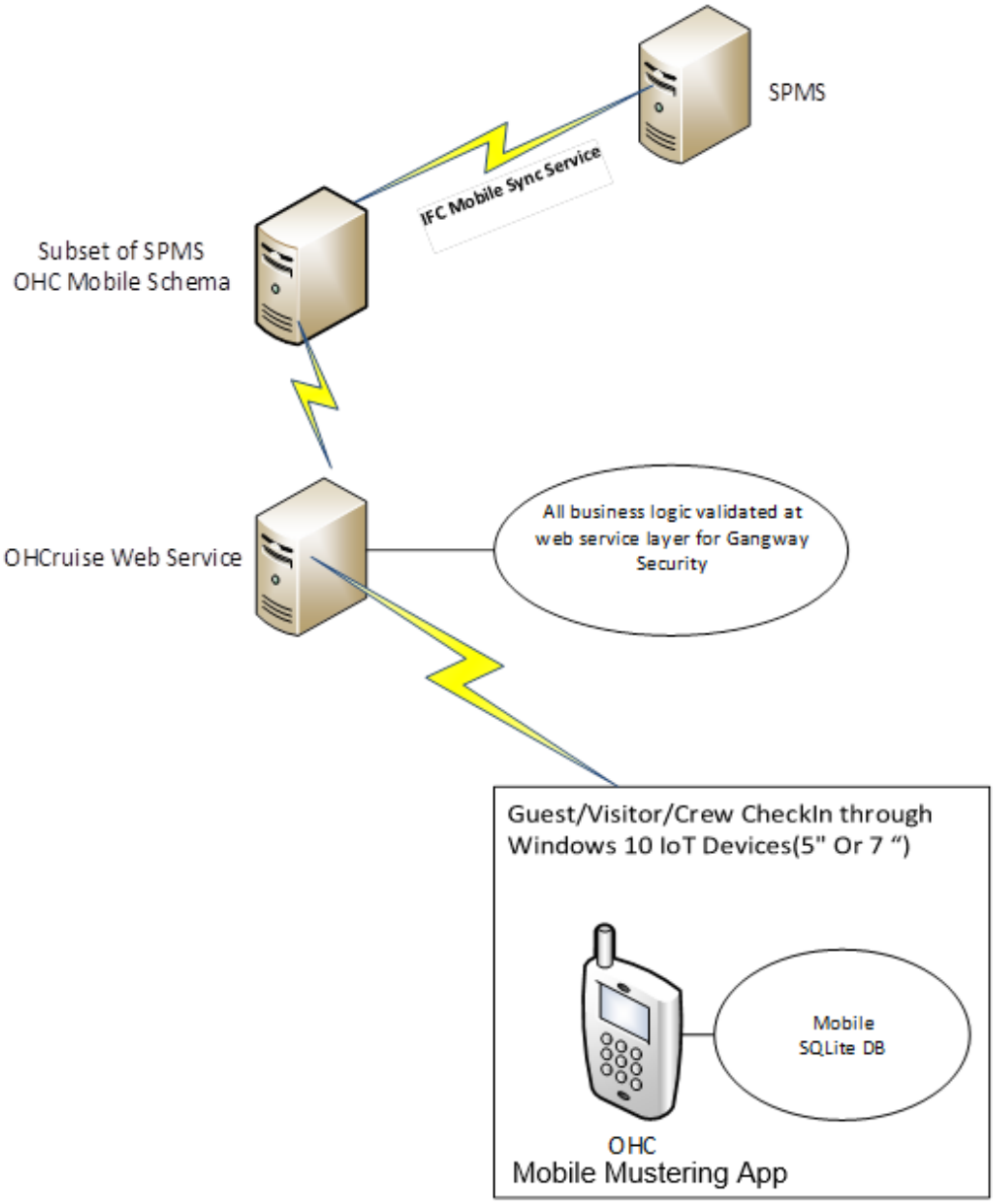


Figure 1-2 Mobile Mustering System Schematic



2
System Configuration

This section describes the configuration required before you can start using the Mobile Mustering application. Configuration includes setting up of the Application Server for Mobile applications, Mobile Sync Interface, and Windows 10 Mobile/Tablet.

FC Mobile Database Preparation

Apart from storing the existing Muster Station information such as passengers, crews, and visitor details in the SPMS Database, a separate database is required for Mobile Mustering to store the essential information for its mobile devices, and this database may reside on the same server as SPMS Database.

You must create the FCMobile Schema. Use the following script:

```
CREATE USER fcmobile IDENTIFIED BY <password>
DEFAULT TABLESPACE USER_TABLES TEMPORARY TABLESPACE USER_TEMP;
GRANT CONNECT TO fcmobile;
GRANT DBA TO fcmobile;
```

To create the database tables for the FCMobile Schema, you must perform a database verification on the MobileSync program. See Configuring Mobile Sync Interface for more details on Interface setup and database synchronization.

Setting Up Mobile Application Server

Install the Mobile Application Server involves several components, and you can install in the order as described in the following section.

Turning on Microsoft Windows IIS Feature

You must turn on the IIS Feature to allow the Application Server to communicate with the World Wide Web Services.

1. In Windows Server, access the **Control Panel, Programs** and **Features**.
2. Select **Turn Windows features on or off**.
3. On the **Internet Information Services**, expand the **World Wide Web Services** container.
4. Ensure the **ASP.NET** and **CGI** checkboxes are selected. If not, select the respective checkbox and click **OK**.

.NET Framework

The OHCruiseWeb Service requires a version of .NET Framework 4.0 installed. Verify the version is installed on your Application Server by navigating to **Control Panel, Programs and Features, Add Remove Software** section. If you do not have a .NET Framework 4.0

installed, download a copy of the installation file from the Microsoft website and manually run the offline Microsoft .NET Framework 4.0 Installer.

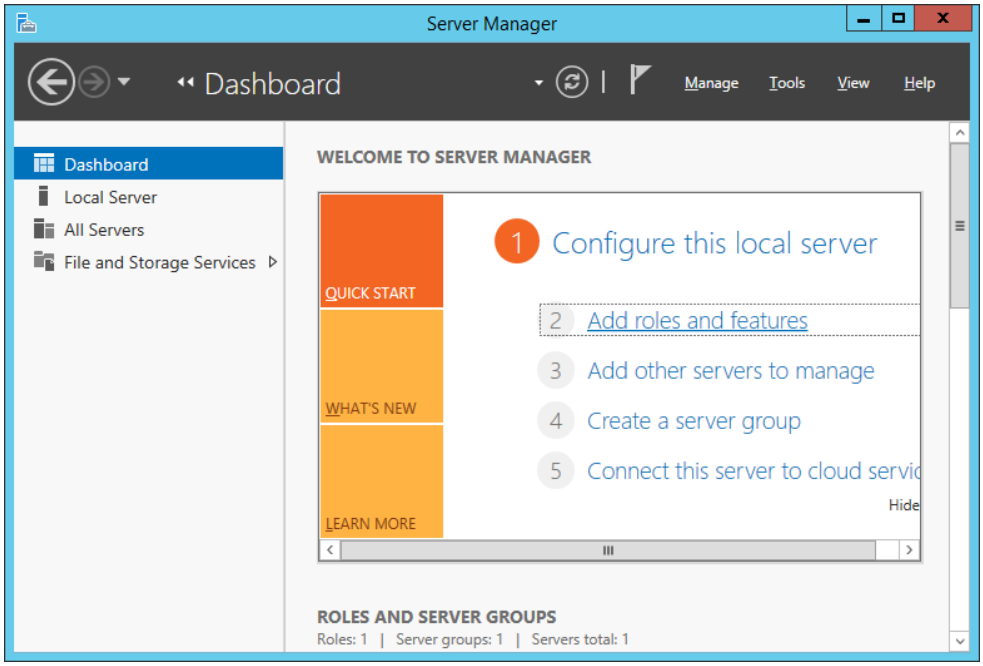
Oracle ODAC and Instant Client

You must have both the Oracle ODAC and Instant Client installed on the Application Server. Refer to Oracle Technology Network (OTN) website at http://www.oracle.com/technetwork/topics/dotnet/downloads/install112030-1440546.html and download the version listed in the Prerequisites. You do not have to uninstall the ODAC that you previously installed.

Adding Roles to Microsoft Windows Server 2012 R2

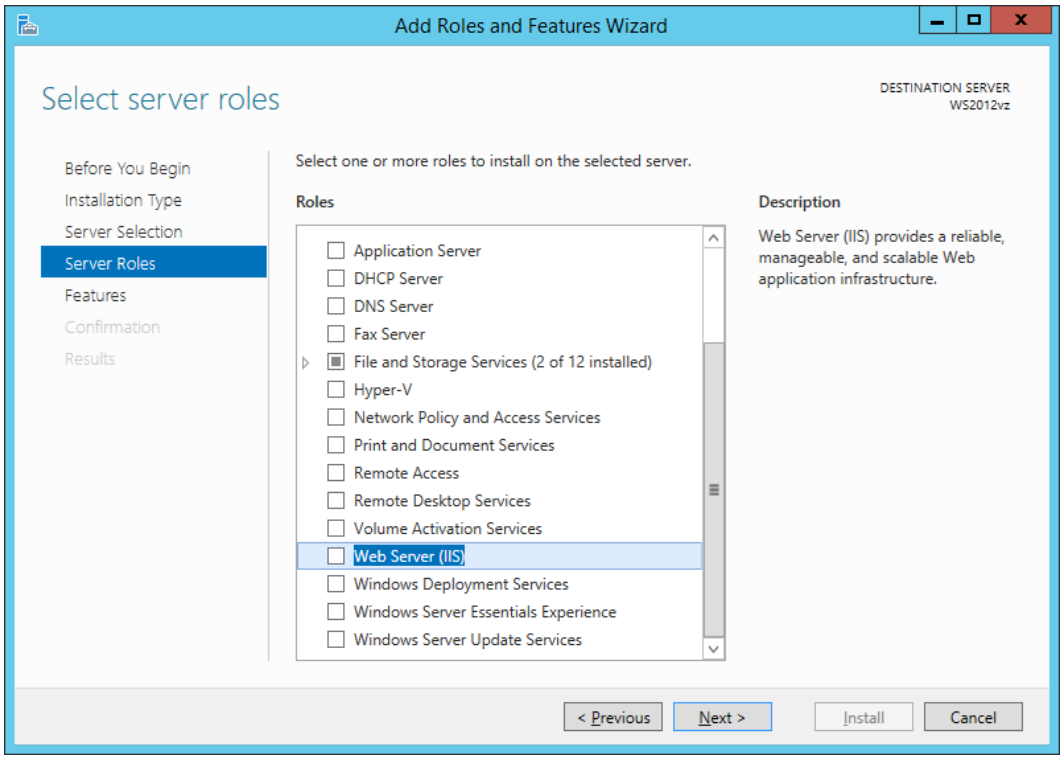
1. On the Server Manager Dashboard, click **Roles** and select **Add Roles**.

Figure 2-1 Mobile Server Dashboard



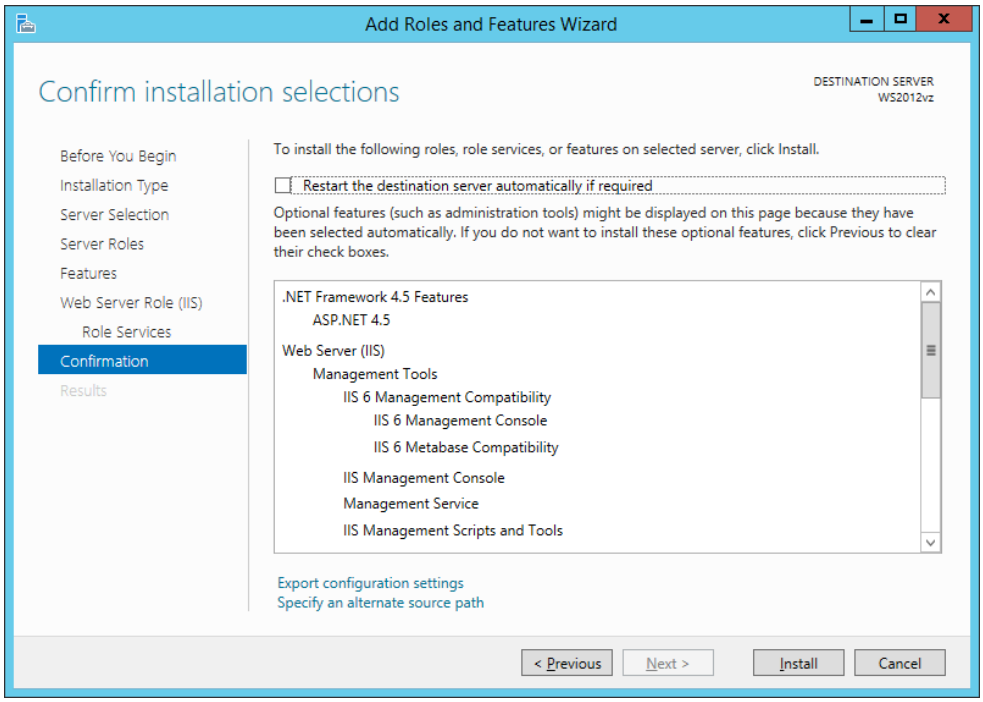
2. On the Before You Begin page, make sure that the criteria listed on the page are met.
3. Navigate to the Installation Type page and select the **Role-based** or **feature-based installation**.
4. On the Server Selection section, select the **server** from the server pool option.
5. On the Select Server Roles section, select the **File Services** and **Web Service (IIS)** component checkbox.

Figure 2-2 Server Roles Ffor Web Server (IIS)



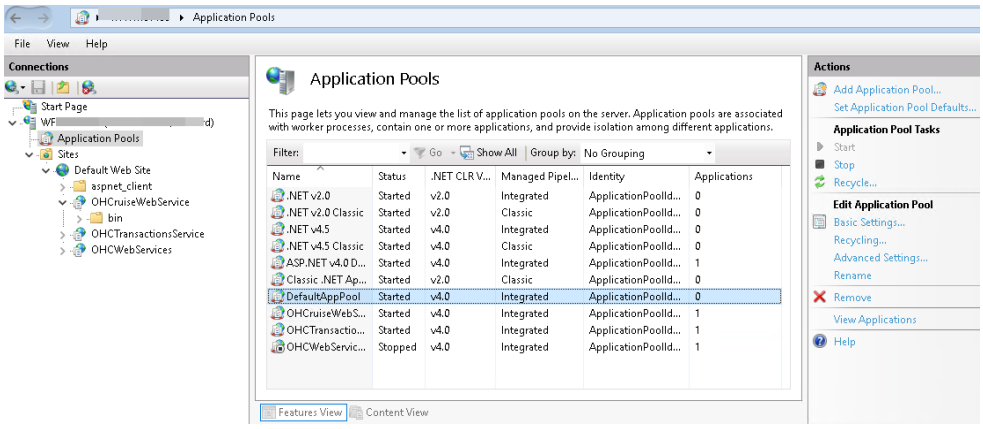
6. On the Features section, select the **.NET Framework 4.0**.
7. On the Web Server Role window, select **Management Tools, Common Http Features, Application Development, IIS 6.0 Management Tools**, click **Next**, and follow the steps of the Installation Wizard.
8. On the Confirmation Window, select the **Restart the destination server automatically if required** and click the **Install** button.

Figure 2-3 Roles And Features Confirmation



9. From the Server Manager container, select **Internet Information Services (IIS) Manager**, and then select **Application Pools, DefaultAppPool**.
10. Select **Edit Application Pool, Advance Settings** from the **Action Panel** and change the **.NET CLR version** to **v4.0**.

Figure 2-4 IIS Manager Application Pools



Verifying the SSL Connection

Run the following steps to ensure the SSL connection is properly set up:

1. From the Application Server, navigate to the Server Manager window and select **IIS Manager, Default Web Site**.
2. On the Actions pane on the left, under Edit Site, select **Bindings**.

3. On the Site Bindings window, select **Add**.
4. Enter the **Port Number** in the Add Site Binding. The default port is 80.
5. On the **Default Web Site, OHCruiseWebService** select **Directory Browsing**, and then click **Enable** on the **Actions** pane.

Setting Up OHCWebServices

1. Launch the **OHCruiseWebservice.msi** file and follow the installation steps.
2. On the OHCruiseWebservice, InstallShield Wizard, select the set up type **Complete**.
3. Click **Next** and follow the installation steps until completion.
4. The OHCruiseWebservice is listed under the Default Web Site of the IIS Manager, Connection section once the setup is complete.
5. From the Server Manager, Sites container, select **OHCruiseWebService** and navigate to Actions Panel and select **Advance Settings**.
6. Ensure the Enable 32–Bit Applications is set to True and .Net CLR version is set to v4.0.
7. In the Default Web Site, OHCruiseWebService, select **Directory Browsing** and then select **Enable** from the Actions Panel on the right.

Configuring DB Source

1. On the IIS Manager, Connection branch, right-click the OHCruiseWebservice and select Explore. This opens the `C:\inetpub\wwwroot\OHCruiseWebService` folder.
2. Locate the Web.Config file and edit the connection string to point the connection to the correct Data Source.

```
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvider">
<add name="MyLocalOracleServer" connectionString="Data
Source=spms;Persist Security Info=True;User
ID=fcmobile;Password=<password>;"
providerName="System.Data.OracleClient"/>
</connectionStrings>
```

Encrypting Web.config File

As an alternative, it is possible to encrypt and decrypt the Web.config file using a script.

1. Open the Command Prompt with Run as Administrators.
2. Change the directory to `"%WinDir%\Microsoft.NET\Framework\v4.0.30319"`.
3. Run the below command to encrypt the connection string.

```
<connectionString> aspnet_regiis -pe "connectionStrings" -app "/
OHCruiseWebService" -prov "DataProtectionConfigurationProvider"
```

The above command with the app switch assumes that there is an IIS Virtual directory called OHCruiseWebService and the command below assumes there is no virtual directory available.

```
Encrypting configuration section... Succeeded!
```

To Change the connection strings section back to clear text, run the following command from the command prompt.

```
aspnet_regiis -pd "connectionStrings" -app "/OHCruiseWebService"
```

If the command is successful, you will see the following output:

```
Decrypting configuration section... Succeeded!
```

To decrypt the connection Strings section specifying a physical path to your application's configuration file, use the -pdf switch as shown here.

```
aspnet_regiis -pdf "connectionStrings"<DIR>\ OHCruiseWebService
```

Verifying WebServices Connection

To ensure the WebService connection is properly set up:

1. Open a web browser from the machine where the web service is installed.
2. Copy and paste the following URL into your browser.

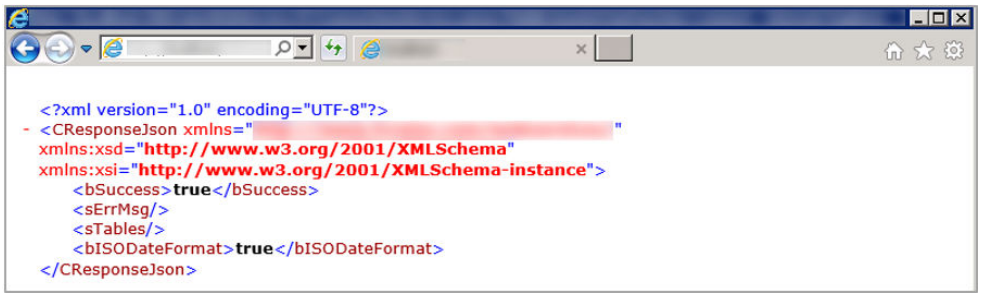
   http://localhost/OHCruiseWebService/FCTransactionsService.asmx/MobileJsonGet?psFunction=connect&psSessionID=&psParam=&pbIsSelect=false&psSchemaName=

   You should get the following respond from the browser.

```
<CResponseJson><bSuccess>true</bSuccess><sTables/
><bISODateFormat>true</bISODateFormat></CResponseJson>
```

If the Web Service is configured correctly, the following page is shown.

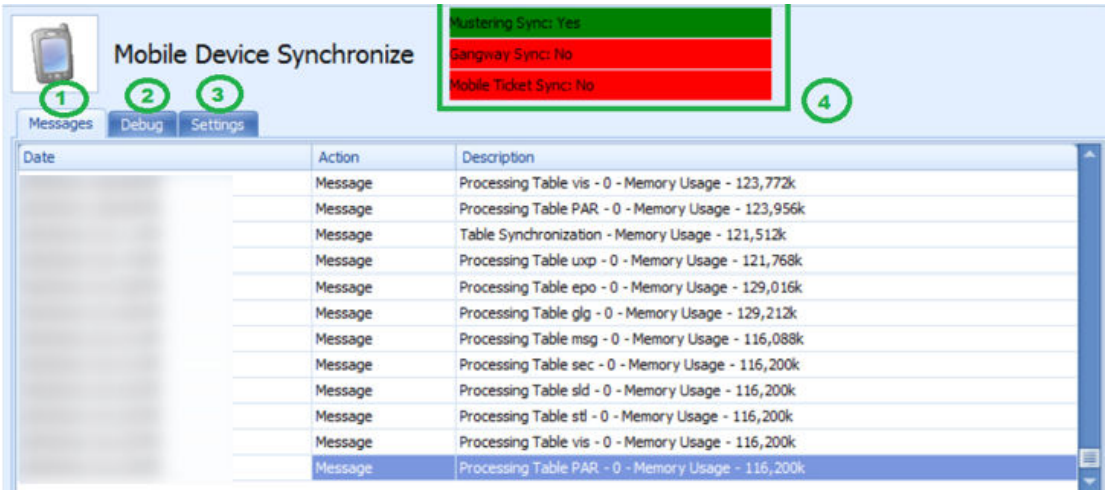
Figure 2-5 WebService Connection Response Page



Setting up Mobile Sync Interface

The MobileSync Interface is a program that synchronizes the data between the SPMS and the Mobile database based on the interval time configured in the **OHC MobileSync Interface**.

Figure 2-6 Mobile Sync Interface



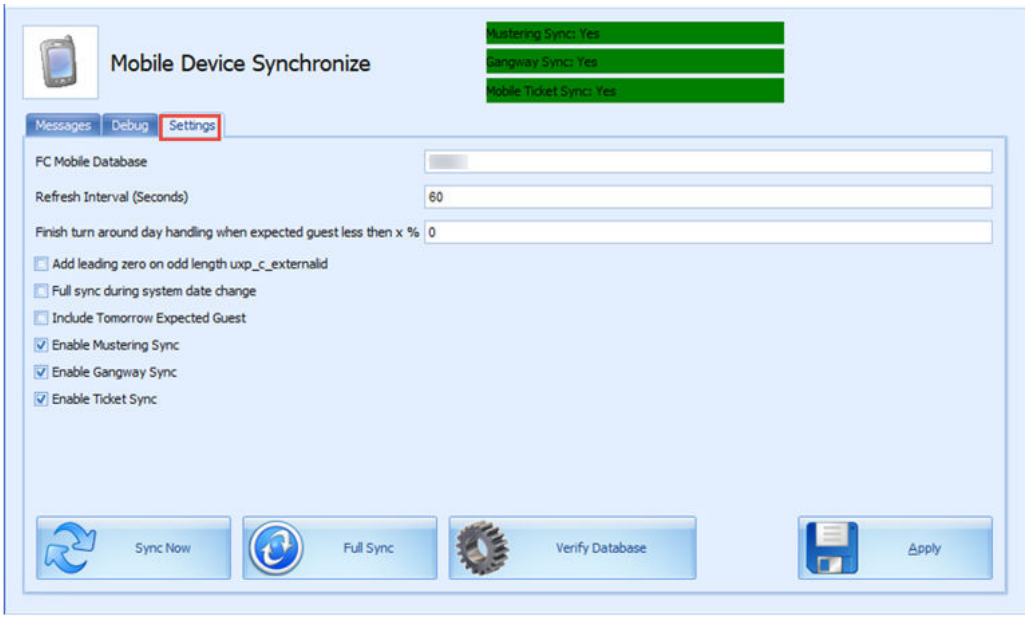
1. Tab lists all synchronization activities.
2. Tab presents all activities in debugging format with SQL Command.
3. Tab defines the required settings and synchronization functions.
4. Labels indicating the type of synchronization enabled within the Settings tab.

Ensure the SPMS Database parameter table field ‘PAR_SYNC_TO_MOBILE’ value is set to 1. For list of parameters and settings required by the MobileSync Interface, see topic Parameters.

Configuring Mobile Sync Interface

The data between the Ship and FCMobile database will synchronize smoothly when the interface is correctly set up.

Figure 2-7 OHCMobile Sync Settings



1. Run the **Mobile Sync.exe** and navigate to the Settings tab.
2. Enter the Mobile DB name in the FC Mobile Database name field, similar to the one defined in Oracle Net Manager.
3. The synchronization between the databases is based on the time entered in **Refresh Interval Seconds**. The default Refresh Interval (Seconds) is 60 seconds.
4. Click **Apply** to save. The settings are saved in the **OHCSettings.par** file.

Table 2-1 Field Definition of Mobile Sync Interface

Field Name	Description
Refresh Interval (Seconds)	Triggers synchronization automatically according to the pre-defined seconds. The default is 60 seconds.
Enable Turn Around Day Handling	This function adds a message to **CHG_MOBILE_IN** table, signifying the turnaround day. • If the system date change matches the cruise start date, message **'START_TURNAROUND_DAY'** will be written to the CHG_MOBILE_IN table. • If **'Expected Check-In guest < %'** as per setup in MobileSync Setting, message **'END_TURNAROUND_DAY'** will be written to the CHG_MOBILE_IN table. • If **'Expected Check-In guest > %'** as per setup and if current System Cruise changed, message **'END_TURNAROUND_DAY'** will be written to the CHG_MOBILE_IN table.

Table 2-1 (Cont.) Field Definition of Mobile Sync Interface

Field Name	Description
Add leading zero on odd length uxp_c_externalid	This function adds leading zero to the `UXP_C_EXTERNALID` (Odd length) in FCMOBILE DB whenever a full synchronization is performed.
Full Sync during system date change	This function automatically triggers a Full Synchronization during system date change.
Include Tomorrow Expected Guest	This function includes passenger departing the next day into synchronization.
Enable Mustering Sync	This function enables the synchronization process for Mobile Mustering application.
Enable Gangway Sync	This function enables the synchronization process for Mobile Gangway application.
Enable Ticket Sync	This function enables the synchronization process for Mobile Ticket application.
Sync Now	The Sync Now is an on-demand synchronization process that checks for any record change that requires updating in `CHG_MOBILE_OUT` in Mobile database to Ship database, followed by `CHG_MOBILE_IN` in Ship database to Mobile database.
Full Sync	The Full Sync triggers synchronization between `FCMOBILE_DB` with the Ship database. It truncates the `FCMOBILE_DB` before updating it with the latest data from the Ship database.
Verify Database	The Verify Database updates the `FCMOBILE_DB` structure with the latest version. The system verifies the version in **FCMOBILE.PAR.MOBILE.MOBILE.DB** and if it is found to be out of date, it prompts a warning '**Please Run Verify database first**' before Full Synchronization can be performed.

Creating FCMobile Schema

At the creation of the FCMobile User in Database Preparation, the system requires you to run a database verification and creates the missing data tables in FCMobile Schema. This task can be performed only by the user who has the **Allow Run Verify Database** permission.

Synchronizing the Database

There are two types of synchronization: on demand or full synchronization, which truncates the database.

To perform a synchronization,

1. On the Mobile Sync Interface, Settings tab, verify that the **FC Mobile Database** points to the correct ship database. If not, correct the database name and click **Apply** to save the changes.
2. Select **Sync Now** to immediately perform the synchronization.
3. If the Parameter Mobile, Mobile DB Version value is not the same in Fidelio and FCMobile Schema, the system prompts that you verify the database before it allows you to continue. Only user with the **Allow Run Verify Database** privilege access is allowed to perform this task. Click the **Verify Database** to update the FCMOBILE.DB structure to the latest version.
4. The system writes into the system log *"Run Verify Database – Completed"* at the end of the verification process. This message is also shown on the Message tab before synchronization commences.

Performing a Full Synchronization

The **Full Sync** not only truncates the data and photo from the FCMobile Database before synchronizing, it also purges all pending changes that exist in the database.

> **Important:**
>
> Perform with caution.

1. On the **Mobile Sync Interface, Settings** tab, verify that the **FC Mobile Database** points to the correct ship database. If not, correct the database name and click **Apply** to save the changes.
2. If there are changes pending from the Mobile DB to the Database, the system prompts a warning message. Click **Yes** to delete all pending changes or **No** to cancel the Full Sync process.
3. If you clicked **Yes**, enter the **login ID and password** when prompted.
4. Navigate to the **Message** tab to view the progress. Ensure that the tables are synchronized without any errors.

SPMS Configuration Codes

Before you begin using the Gangway Security and Mobile Mustering function, you must configure the codes in the SPMS Administration module. See Administration User Guide on how to set up these codes.

- Life Boat and Life Raft
- Muster Station
- Stateroom setup

3
Setting Up Mobile Device

The following section describes the setup of Microsoft Windows 10 Mobile devices/Tablets for use onboard the ship.

Installing an Application

1. Right click the **Add-AppDevPackage.ps1** and select **Run with PowerShell.**
2. Follow the installation steps presented.
3. Select **A- Yes to All** and press the **Enter** key to proceed with the installation.
4. Press the **Enter** key to close the PowerShell application once the installation is successful You should see the OHC Mustering application in Windows Programs.

Uninstalling an Application

Before you uninstall the application, ensure that it is not running. Uninstalling a running application will cause issues when you try to reinstall it at a later stage.

1. Go to **Windows Programs, OHC Mustering**.
2. Right-click and select **Uninstall** .
3. At the prompt, click the **Uninstall** button

Connecting Mobile Devices to a PC

After downloading the application onto the mobile device, and launching the application for the first time, the Device Server Setting Screen appears. As an Administrator, you should set the correct **Mobile Web Service Host name** and **Port number**, and then tap on **Connect.**

Once the connection to the Mobile Server is established, a Device Registration screen will prompt. On the Device Registration screen, do the following:

1. Select the appropriate **MAC ID** from the drop-down list.
2. Enter the **Device Name** and the click the **Active & Register** button to activate and register the device to the MOB table.

If registration of the device is successful, the application loads and creates the database in a SQLite DB file and downloads the required tables and data from the Mobile Schema to the SQLite DB.

- Application binaries are installed into folder `C:\Users\xxx\AppData\Local\Packages\af9e2835-d828-441e-acef-3b74d389fb04_ygkypzx4b378t\LocalState`
- Application logs are located into folder `C:\Users\xxx\AppData\Local\Packages\af9e2835-d828-441e-acef-3b74d389fb04_ygkypzx4b378t\LocalState\Log - ddmmyyyy.txt`
- All photos are located into folder `C:\Users\xxx\AppData\Local\Packages\af9e2835-d828-441e-acef-3b74d389fb04_ygkypzx4b378t\LocalState\ProfilePhotoFolder`

- Database is located in the folder `C:\Users\xxx\AppData\Local\Packages\af9e2835-d828-441e-acef-3b74d389fb04_ygkypzx4b378t\LocalState\MusteringDB.sqlitezz`

4
User Security

This section describes the permission access for the MobileSync Interface and Mobile Mustering Module. These security privileges are assigned through the User Security module.

Table 4-1 Mobile Sync Interface User Rights

Security Reference No	Description
4543	Allow Run Verify Database.
3174	Allow Run Full Sync.
3173	Allow Shut Down MobileSync Application.

5
Parameters

This section describes the Parameters available to the Mobile Mustering module, and is accessible from the Administration module under **System Setup, Parameter.**

Table 5-1 PAR_GROUP_MOBILE

PAR Name	PAR Value	Description
Allow Crew Card Login Bypass	0 or 1	Allow login using crew card scanning as long as crew credential is valid in Mobile DB.
Allow to check-in RE/RR person when onboard	0 or 1	Allow to check-in reservation status that is 'RE'/'RE' when the person is onboard
Check-In Status	0,1 or 2	Different Handling for `RES_OFFBOARD` status upon checked-in 0 - Onboard after check-in 1 - Ashore after check-in, must swiped card to be onboard 2 - Display option box
Enable Mobile Data Sync	0 or 1	0 – Disable 1 - Enable Mobile Data Sync to FCMobile DB
FC Mobile Gangway Client Version	E.g: 8.0.1	Mobile Gangway Client Version
FC Mobile Gangway Client Version Major	0 or 1	Mobile Gangway Major Version 0 - Minor Update 1 - Major Update
FC Mobile Gangway update type	1	FC Mobile Gangway update type
Last Update Date/Time	Example: 20130925122924	Last Sync Date and Time in ISO format
Mobile DB Version	E.g: 7.30.8xx	Mobile DB Version
Offline Timeout	Example: 6	Number of hours allowed to use in offline mode before sync is required
Open Login Enabled	0 or 1	0 - Must use correct login details 1 - Allow Open Login/Blind Login

Table 5-1 (Cont.) PAR_GROUP_MOBILE

PAR Name	PAR Value	Description
Require mandatory fields	0 or 1	0-Do not require mandatory field 1-Require mandatory field
Refresh Interval	60	Interval time before the next DB synchronization. The default value is 60 seconds.
Use System Date	0 or 1	0 - Use Device Date 1 - Use System Date

Table 5-2 PAR_GROUP_GANGWAY

PAR Name	PAR Value	Description
Allow not expected guest to Check-In	0 or 1	0 - Do not allow not expected guest to Check-In 1 - Allow not expected guest to Check-In
Not allow to check-in Guest if no photo found	0 or 1	0 - Allow guest to check-in without a photo taken 1 - Do not allow guest to check-in if no photo found