Oracle® Hospitality Cruise Shipboard Property Management System
Gangway Security and Mobile Musterig
Installation Guide
Release 7.30.874
E89108-04

September 2018
Copyright © 2017, 2018, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on 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. 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.
Contents

Tables ................................................................................................................................. 5
Figures ................................................................................................................................. 6
Preface ................................................................................................................................ 7
Audience .............................................................................................................................. 7
Customer Support ............................................................................................................. 7
Revision History .................................................................................................................. 7
Prerequisites, Supported Systems, and Compatibility ....................................................... 8
Prerequisites ....................................................................................................................... 8
Supported Operating Systems ........................................................................................... 8
Supported Hardware .......................................................................................................... 8
Compatibility ....................................................................................................................... 8
1 System Schematic ........................................................................................................... 9
2 System Configuration ..................................................................................................... 11
  2.1. FCMobile Database Preparation .............................................................................. 11
  2.2. Mobile Application Server ....................................................................................... 11
      Turning on Microsoft Windows IIS Feature ................................................................. 11
      .NET Framework ......................................................................................................... 12
      Oracle ODAC and Instant Client .................................................................................. 12
      Adding Roles to Microsoft Windows Server 2008 R2 .................................................. 12
      Adding Roles to Microsoft Windows Server 2012 R2 .................................................. 16
      Install OHCruise Web Service ..................................................................................... 20
      Verifying the Connection without SSL ......................................................................... 21
  2.3. Configure OHCruise Web Services ........................................................................... 22
      Configuring DB Source for the Web Services ............................................................... 22
      Encrypting Web.config file using Command Prompt ..................................................... 23
      Verifying the WebServices connection ....................................................................... 24
  2.4. Oracle Hospitality Cruise SPMS Setup .................................................................... 24
      Life Boat/ Life Raft Setup .............................................................................................. 25
      Muster Station Setup .................................................................................................... 26
      Cabin Setup .................................................................................................................. 26
  2.5. MobileSync Interface ............................................................................................... 27
      Configuring MobileSync Interface .............................................................................. 27
      Creating FCMobile Schema ........................................................................................ 29
      Database Synchronization ............................................................................................ 29
      Performing a Synchronization ....................................................................................... 30
      Performing a Full Synchronization ............................................................................... 30
3 Setting up Mobile Device ................................................................................................. 32
  3.1. Connecting Mobile Devices to PC .......................................................................... 32
3.2. Turn on device discovery and pairing .......................................................... 32
3.3. Connecting to Device Portal ......................................................................... 33
3.4. Windows Device Portal .................................................................................. 34
   Apps Manager ................................................................................................. 34
   Installing an Application ................................................................................... 35
   Uninstalling an Application .............................................................................. 35

4 User Security Group ......................................................................................... 36

Appendix A. Parameters ....................................................................................... 37
   PAR_GROUP MOBILE ...................................................................................... 37
   PAR_GROUP GANGWAY .................................................................................. 38
Table 2-1 - Function definition of IFC MobileSync ..............................................27
Table 2-2 - Field definition of OHC MobileSync Settings ........................................28
Table 4-1 - MobileSync Interface Access Rights ......................................................36
Table A-1 - PAR Group Mobile .................................................................................37
Table A-2 - PAR Group Gangway ..............................................................................38
Figures

Figure 1-1 - Gangway Security System Schematic ......................................................9
Figure 1-2 – Mobile Mustering System Schematic ......................................................10
Figure 2-1 – Setting up Mobile Mustering/Gangway Security Server Roles ..................12
Figure 2-2 – Adding Server Roles ..............................................................................13
Figure 2-3 - Server Roles selection in Mobile Mustering App Server .............................13
Figure 2-4 – Adding WebServices Roles to Mobile App Server ....................................14
Figure 2-5 - Role Services selection in Mobile App Server ............................................14
Figure 2-6 - Adding Features to Mobile App Server .....................................................15
Figure 2-7 - Features selection in Mobile Mustering App Server .................................15
Figure 2-8 - Enabling Advance Settings in IIS ............................................................16
Figure 2-9 - IIS Advance Setting ..................................................................................16
Figure 2-10 – Mobile Server Roles .............................................................................17
Figure 2-11 - Mobile Server Web Server (IIS) .............................................................17
Figure 2-12 - Application Server confirmation screen ..................................................18
Figure 2-13 - Enabling Advance Settings in IIS ..........................................................18
Figure 2-14 - IIS Advance Setting ................................................................................19
Figure 2-15 - Edit Site Binding .....................................................................................19
Figure 2-16 - IIS MIME Types ......................................................................................20
Figure 2-17 - IIS Services ............................................................................................21
Figure 2-18 - Enabling SSL Settings ..........................................................................21
Figure 2-19 - Enabling Directory Browsing .................................................................22
Figure 2-20 - IIS Services ............................................................................................22
Figure 2-21 - Verifying Webservices connection .........................................................24
Figure 2-22 - Adding Lifeboat/LifeRaft ....................................................................25
Figure 2-23 - Adding Muster Station .........................................................................26
Figure 2-24 - LifeBoat, Muster Station, Location and Vertical Zone assignment ............26
Figure 2-25 - IFC MobileSync Interface screen ............................................................27
Figure 2-26 - OHC MobileSync Settings .................................................................28
Figure 2-27 - OHC MobileSync Settings page ..........................................................30
Figure 2-28 – Synchronized tables in OHC MobileSync .............................................31
Figure 3-1 - Windows Update & Security .................................................................32
Figure 3-2 - Turn On Device Discovery ....................................................................33
Figure 3-3 - Connect Using .......................................................................................34
Figure 3-4 - Windows Device Portal ...........................................................................34
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 function is to process passenger and crew embarkation, administer movement through the Gangway using a Microsoft Windows 10 Mobile/Tablet.

This document describes the full setup of the Mobile Application Server, Mobile Gangway client on mobile devices and the SPMS System Configuration.

Audience

This document is intended for application specialist, IT Officers and end-users of Oracle Hospitality Cruise Shipboard Property Management System.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL: https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2017</td>
<td>Initial publication.</td>
</tr>
<tr>
<td>December 2017</td>
<td>Changed method of encryption using a Command Prompt.</td>
</tr>
<tr>
<td>May 2018</td>
<td>Log SQL feature were removed</td>
</tr>
<tr>
<td>June 2018</td>
<td>Hardcoded passwords/keys were removed</td>
</tr>
<tr>
<td>September 2018</td>
<td>Revised .NET Setup</td>
</tr>
</tbody>
</table>
Prerequisites, Supported Systems, and Compatibility

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

Prerequisites

- FCMobile Database
- OHCruiseWebService.7z
- Cabin Station Setup
- Application Server for Mobile Services.
- Preinstalled Oracle Data Access Component (ODAC) for PC running SPMS applications.
  - ODTwithODAC112030 or
  - ODTwithODAC121021

Supported Operating Systems

- Microsoft Windows 10 IoT
- Microsoft Windows Server 2008 R2 Standard OS
- Microsoft Windows Server 2012 R2 Standard OS

Supported Hardware

- Oracle MICROS 720 Tablet
- Oracle MICROS 721 Tablet
- Windows Mobile device with a camera.
- Server based CPU (Xeon X3440 2.53 GHz)
- Minimum RAM: 8 GB

Compatibility

SPMS version 7.30.874 or later. For customers operating on version 7.30.874 and below, database upgrade to the recommended or latest version is required.
The Gangway Security and Mobile Mustering application consist of several components, and these components are responsible for transmitting information between the mobile device and the SPMS database. Below diagrams further illustrate the schematic flow between these components.

**Figure 1-1 - Gangway Security System Schematic**
Figure 1-2 – Mobile Mustering System Schematic
2 System Configuration

This section describes the required configuration prior to using the Mobile Mustering application, including setting up of Application Server for Mobile applications, MobileSync Interface and Windows 10 Mobile/Tablet.

2.1. FCMobile Database Preparation

Apart from storing the existing Muster Station information such as passengers, crews and visitors 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.

The FCMobile Schema User must be created using below script.

```
CREATE USER fcmobile
IDENTIFIED BY <password>
DEFAULT TABLESPACE USER_TABLES
TEMPORARY TABLESPACE USER_TEMP;

GRANT CONNECT TO fcmobile;
GRANT DBA TO fcmobile;
```

In order to create the database tables for FCMobile Schema, a database verification must be performed on MobileSync program. Refer Configuring MobileSync Interface for more details on Interface setup and database synchronization.

2.2. Mobile Application Server

The installation of Mobile Application Server involves several components, and installation must be done in the order as described in below section.

Turning on Microsoft Windows IIS Feature

The Application Server would require the IIS feature to be turned on for communication with the World Wide Web Services.

1. In Windows Server, access the Control Panel, Programs and Features and select Turn Windows features on or off.
2. Under the Internet Information Services, expand the World Wide Web Services container and ensure the ASP.NET and CGI check box is checked. If not, please select the respective check box and then click OK.
.NET Framework

The OHCruiseWeb Service requires a version of .NET Framework 4.0 to be installed. You can verify if 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 https://www.microsoft.com/en-us/download/developer-tools.aspx and manually run the offline Microsoft .NET Framework 4.0 Installer.

Oracle ODAC and Instant Client

An Oracle ODAC and Instant Client must be 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 Prerequisites. If an ODAC is installed previously, de-installation is not required.

Adding Roles to Microsoft Windows Server 2008 R2

1. In the Server Manager container, click Roles and then select Add Roles.

   ![Figure 2-1 – Setting up Mobile Mustering/Gangway Security Server Roles](image)

2. In Before You Begin page, check that the criterion listed on the page are met before continuing.
3. In the Select Server Roles page, select the **File Services and Web Server (IIS)** component check box, and then click **Install**.

4. At the end of the components installation, select the **Web Server (IIS)** from the Server Manager container, and then select **Add Role Services**.
5. In Select Role Services page, place a check mark in Management Tools, Common HTTP Features, Application Development, IIS 6.0 Management, and then click Install.

6. Select the .NET Framework 4.0 and then select Add Features from the Server Manager container.
7. In Select Features screen, select the .Net Framework 4.0 Features and Windows Process Activation Service check box, and then click Install.
8. From the Server Manager container, select Internet Information Services (IIS) Manager, then Application Pools, DefaultAppPool, and then Advance Settings.

![Figure 2-8 - Enabling Advance Settings in IIS](image)

9. Ensure the Enable 32-Bit Applications is set to True.

![Figure 2-9 - IIS Advance Setting](image)

**Adding Roles to Microsoft Windows Server 2012 R2**

1. In the Server Manager Dashboard, click Roles and select Add Roles.
2. In Before You Begin page, check that the criteria’s listed on the page are met before continuing, then navigate to the Installation Type page and select the **Role-based or feature-based installation**.

3. In the Server Selection section, select the server from the server pool option.

4. In the Select Server Roles section, select the **File Services and Web Server (IIS)** component check box.

5. In the Features section, select the **.NET Framework 4.0**.

6. In the Web Server Role screen, select **Management Tools, Common Http Features, Application Development, IIS 6.0 Management Tools**, then click **Next** and follow the steps of the Installation Wizard.
7. In the Confirmation Screen, check the Restart the destination server automatically if required and then click the Install button.

![Application Server confirmation screen](image)

**Figure 2-12 - Application Server confirmation screen**

8. From the Server Manager container, select Internet Information Services (IIS) Manager, then Application Pools, OHCruiseWebService-AppPool, and then select Edit Application Pool, Advance Settings from the Action Panel and change the .NET CLR version to v4.0.

![Enabling Advance Settings in IIS](image)

**Figure 2-13 - Enabling Advance Settings in IIS**

9. Ensure the Enable 32-Bit Applications is set to True.
Figure 2-14 - IIS Advance Setting

10. Open the IIS Manager, Default Web Site, Bindings and ensure SSL port using Window default port 80.

Figure 2-15 - Edit Site Binding

11. Open the IIS Manager, IIS Home page, MIME Types and then remove .pak and .cab extensions from the list. Repeat the same for Default Web Site.
Install OHCruise Web Service

1. Launch the OHCruiseWebService.msi application, and then follow installation steps. (Remove point no.1,2 & 3 as it has been moved to above)
2. At the OHCruiseWebService – InstallShield Wizard screen, select the setup type as Complete, click Next and follow the installation steps until completion.
3. At the end of the setup, the OHCCruiseWebService is displayed in the IIS Manager, Connections section.

Verifying the Connection without SSL

To ensure that the SSL connection is properly configured,

1. From the Application Server, navigate to the Server Manager screen. Under the Connections section, expand the Sites container, select Default Web Site, SSL Settings and ensure the 'Require SSL' is unchecked.

2. Select OHCCruiseWebService and then un-check the Require SSL in SSL Settings.

3. Click Apply to save.

4. In the Default Web Site, select Directory Browsing and then select Enable from the Actions Panel on the right.
5. In the Default Web Site, OH CruiseWebService, select Directory Browsing and then select Enable from the Actions Panel on the right.

2.3. Configure OH Cruise Web Services

1. Launch the OH CruiseWebService.msi application, and then follow installation steps.

2. At the OH CruiseWebService – InstallShield Wizard screen, select the setup type as Complete, click Next and follow the installation steps until completion.

3. At the end of the setup, the OH CruiseWebService is displayed in the IIS Manager, Connections section.

Configuring DB Source for the Web Services

1. From the IIS Manager, Connections section, right-click the OH CruiseWebService and select Explore. This opens the folder C:\inetpub\wwwroot\OH CruiseWebService
2. Locate the **Web.Config** file and edit the following section to point to the correct “Data Source” and then **Save** the file.

```xml
<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 using Command Prompt**

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

1. Open **Command Prompt** with Administrator rights.
2. Change directory to “%WinDir%\Microsoft.NET\Framework\v4.0.30319” Directory.
3. Run below command to encrypt connectionString.
   ```bash
   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.

   ```bash
   aspnet_regiis.exe -pef "connectionStrings" C:\Projects\MachineDPAPI ?prov "DataProtectionConfigurationProvider"
   ```

   Encrypting configuration section...
   Succeeded!

   **To change the connectionStrings section back to clear text, run the following command from the command prompt:**

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

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

   Encrypting configuration section...
   Succeeded!

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

   ```bash
   aspnet_regiis -pdf "connectionStrings" C:\Projects\OHCruiseWebService
   ```
Verifying the WebServices connection

To ensure the WebServices connection is properly setup,
1. Open the web browser of the machine where the web service is installed.
2. Copy and paste the following URL into your browser:

   The browser should respond with the following:
   <CResponseJson><bSuccess>true</bSuccess><sTables/><bISODateFormat>true</bISODateFormat></CResponseJson>

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

Figure 2-21 - Verifying Webservices connection

2.4. Oracle Hospitality Cruise SPMS Setup

Other than setting up the hardware and database, the SPMS program would also require some setup of Muster Station, Lifeboat/Life Raft, and Cabins in Administration module, if they are not done. This is to ensure that all passengers and crew onboard are accounted for during an emergency evacuation. It is essential to that all information entered in the Muster Station, Lifeboat and Cabin are correct.
Life Boat/ Life Raft Setup

1. Login to the Administration module, and select Administration from the menu bar.
2. Select Safety Setup, and then Life Boat/Life Raft Setup from the drop-down list.
3. Right-click on the blank field to bring up the dialog box, and then select Add to add new lifeboat.
4. Insert the Description, Capacity and all other relevant fields in the Details section on the right.
5. Click Apply to save settings.
Muster Station Setup

1. Repeat step 1 of LifeBoat/Life Raft Setup.
2. Select Safety Setup, and then Muster Station from the drop-down list.
3. Right-click on the blank field to bring up the dialog box, and then select Add Muster Station to add a new muster station.
4. Insert the Description, Capacity and select the Lifeboat Type for this Muster Station.
5. Click Apply to save settings.
6. To add more Muster stations, repeat the above steps.

Cabin Setup

Figure 2-23 - Adding Muster Station

Figure 2-24 - LifeBoat, Muster Station, Location and Vertical Zone assignment
1. Repeat step 1 of LifeBoat/Life Raft Setup.
2. Select Staterooms Setup, and then Staterooms from the drop-down list.
3. In the Cabin Setup form, select the Cabin number, and then click Edit to open the Edit Cabin form.
4. Assign the LifeBoat/LifeRaft, Muster Station, Location for this cabin, and then click OK to save the assignment.

2.5. MobileSync Interface

The MobileSync Interface is a program that synchronizes the data between the SPMS and the Mobile database, based on the interval time set in the IFC MobileSync Interface.

![MobileSync Interface Screen](image)

### Figure 2-25 - IFC MobileSync Interface screen

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tab indicates all synchronization activities.</td>
</tr>
<tr>
<td>2.</td>
<td>Tab represents all activities in debugging format with SQL Command.</td>
</tr>
<tr>
<td>3.</td>
<td>Tab defines the required settings and synchronization functions.</td>
</tr>
<tr>
<td>4.</td>
<td>Labels that define the types of synchronization enabled from the Settings tab.</td>
</tr>
</tbody>
</table>

### Configuring MobileSync Interface

The data between the Ship and FCMobile database will synchronize seamlessly when the interface is correctly setup.
1. Launch the **MobileSync.exe** and navigate to the **Settings** tab.

2. The default FCMobile Database is ‘*Fidelio*’. Enter the Mobile DB name in **FC Mobile Database name** field, similar to the one defined in Oracle Net Manager.

3. The default Refresh Interval (Seconds) is 60 seconds. Enter the refresh interval to perform the synchronization between these databases in **Refresh Interval Seconds**.

4. Click **Apply** to save. These settings are saved to **FCSettings.par** file.

![MobileSync Settings](image)

**Figure 2-26 - OHC MobileSync Settings**

Below are the Optional functions available in OHC MobileSync Settings:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Interval (Seconds)</td>
<td>Triggers synchronization automatically according to the pre-defined seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>Enable Turn Around Day Handling</td>
<td>This function adds a message to <strong>CHG_MOBILE_IN</strong> table, signifying the turnaround day.</td>
</tr>
<tr>
<td></td>
<td>- If the system date change matches the cruise start date, message ‘START_TURNAROUND_DAY’ will be written to the CHG_MOBILE_IN table.</td>
</tr>
<tr>
<td></td>
<td>- If ‘Expected Check-In guest &lt; %’ as per setup in MobileSync Setting, message ‘END_TURNAROUND_DAY’ will be written to the CHG_MOBILE_IN table.</td>
</tr>
<tr>
<td></td>
<td>- If ‘Expected Check-In guest &gt; %’ as per setup and if current System Cruise changed, message ‘END_TURNAROUND_DAY’ will be written to the CHG_MOBILE_IN table.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Definitions</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Add leading zero on odd length uxp_c_externalid</td>
<td>This function adds leading zero to the UXP_C_EXTERNALID (Odd length) in FCMOBILE DB whenever a full synchronization is performed.</td>
</tr>
<tr>
<td>Full Sync during system date change</td>
<td>This function automatically triggers a Full Synchronization during system date change.</td>
</tr>
<tr>
<td>Include Tomorrow Expected Guest</td>
<td>This function includes passenger departing the next day into synchronization.</td>
</tr>
<tr>
<td>Enable Mustering Sync</td>
<td>This function enables the synchronization process for Mobile Mustering application.</td>
</tr>
<tr>
<td>Enable Gangway Sync</td>
<td>This function enables the synchronization process for Mobile Gangway application.</td>
</tr>
<tr>
<td>Enable Ticket Sync</td>
<td>This function enables the synchronization process for Mobile Ticket application.</td>
</tr>
<tr>
<td>Sync Now</td>
<td>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.</td>
</tr>
<tr>
<td>Full Sync</td>
<td>The Full Sync triggers synchronization between FCMOBILE_DB with the Ship database. It truncates the FCMOBILE_DB prior to updating it with the latest data from Ship database.</td>
</tr>
<tr>
<td>Verify Database</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Creating FCMobile Schema

During the creation of the FCMobile User in Database Preparation, the system requires you to run a database verification and enable the creation of missing data tables in FCMobile Schema. The task requires a user with access rights ‘Allow Run Verify Database’ granted.

## Database Synchronization

An on-demand synchronization may be triggered when the need arises, and this is performed through the MobileSync application.
Performing a Synchronization

1. At the Settings tab of MobileSync application, verify that the FC Mobile Database is pointing to the correct ship database. If not, correct the database name and click Apply to save the changes.

2. Select Sync Now to perform the synchronization immediately.

3. If the parameter Mobile, Mobile DB Version value is not the same in Fidelio and FCMobile Schema, the system prompts for database verification before allowing you to continue. Only a user with access rights ‘Allow Run Verify Database’ is allowed to perform this task. Click the Verify Database located at the bottom of the screen to update the FCMOBILE.DB structure to the latest version.

4. The system inserts a message ‘Run Verify Database – Completed’ into the system log at the end of the verification process and this message is also shown on the Message tab before proceeding with synchronization.

Performing a Full Synchronization

The FULLSYNC process not only truncates data in FCMobile Schema before synchronizing all relevant data and photos from Fidelio Schema to FCMobile Schema, it also purges all pending changes that exist in the database. Perform this function with caution.

---

1 FCMobile Database
2 Sync Now button
3 Verify Database button
1. Repeat step 1 of the above and then select **Full Sync**.
2. If there are pending changes from **Mobile DB** to **Fidelio DB**, the system prompts a warning message. Clicking **Yes** will *wipe out* all pending changes and **No** will cancel the Full Sync process.
3. If **Yes** is clicked, enter the **login ID** and **password** when prompt.
4. To view the synchronization progress, navigate to the **Message** tab. At the end of the synchronization process, ensure the tables are synchronized without any error.

Figure 2-28 – Synchronized tables in OHC MobileSync
3 Setting up Mobile Device

The following section describes the setup Microsoft Windows 10 Mobile device/Tablet.

3.1. Connecting Mobile Devices to PC

The installation of the Mobile Musterling and Gangway Security application would require the Developer Mode of the mobile device to be turned on.

![Windows Update & Security](image)

**Use developer features**

These settings are intended for development use only.

- **Learn more**
- Windows Store apps
  - Only install apps from the Windows Store.
- Sideload apps
  - Install apps from other sources that you trust, like your workplace.
- **Developer mode**
  - Install any signed app and use advanced development features.

**Figure 3-1 - Windows Update & Security**

1. Press the **Windows + I** keys simultaneously on the mobile device to open the **Settings** window.
2. Select **Update & Security**.
3. On the left of the screen, click **For Developers**.
4. Under “Use developer features” select the **Developer mode** option.
5. Restart the computer/mobile device.

3.2. Turn on device discovery and pairing

To connect to Device Portal, the Device Discovery and Device Portal must be enabled in your phone's settings. This enables you to pair your phone with a PC or other Microsoft Windows 10 device. Both the devices must be connected to the same subnet of the network by a wired or wireless connection or they must be connected by USB. When connecting the device to the Device Portal for the first time, you are required to enter a 6-characters security code and this code is **case-sensitive**. This is to ensure that you have access to the phone and are safe from attackers.

Tap the **Pair** button on your phone to generate and display the code, and then enter the 6-characters into the text box of the browser. Ensure the device/tablet WI-FI is enabled and connected to a WI-FI network.
3.3. Connecting to Device Portal

To establish the connection to the Device Portal, launch a browser and enter the address shown below for the connection type you are using.

- **USB:** [http://127.0.0.1:10080](http://127.0.0.1:10080)
  
  Use this address when the phone is connected to a PC via a USB connection. Both devices platform must be a Microsoft Windows 10.

- **Local Network:** [https://<The IP address or hostname of the phone>](https://<The IP address or hostname of the phone>)

  Use this address to connect to a local network.

  The IP address of the phone is shown in the Device Portal settings on the phone. An HTTPS connection is required for authentication and secure communication. The hostname in **Settings, System, About page** can also be used to access the Device Portal on the local network. For example, [http://Phone360](http://Phone360). This is useful for devices that change their networks or IP addresses frequently, or need to be shared.
3.4. Windows Device Portal

Your Device Portal session starts at the home page. The home page typically has information about the device, such as name and OS version, and preferences that you can set for the device.

Apps Manager

The Apps Manager provides the install/uninstall and management functionality for AppX packages and bundles on your device.
Setting up Mobile Device

- **Install app**: Function allows you to select an application package for installation from a folder on your computer or network.
- **Dependency**: Adds dependencies to the application you are going to install.
- **Deploy**: Deploy the selected app and dependencies to your device.
- **Installed apps**: Function Removes or Start an application.
- **Running apps**: Lists applications that are running currently and provides the option to close them.

## Installing an Application

1. Under the Install app section, click **Browse** and locate the application package (.appx), and then click **Browse** and locate the certificate file (.cer). This is not required on all devices.
2. Click **Add dependencies** if you have more than one. Add each dependency individually.
3. Under **Deploy**, click **Go**.
4. To install another app, click the **Reset** button to clear the fields and repeat the steps.

## Uninstalling an Application

Before you uninstall the application, ensure that your application is not running.

1. Go to **Running apps** section and check the status of the application.
2. If the application found to be running, click the X to close it.
3. Uninstalling a running application will cause issues when trying to re-install the application at a later stage. Once ready, click **Uninstall**.
This section describes the access rights permissible to access the MobileSync Interface and Mobile Mustering Module. These security privileges are assigned through the User Security module.

Table 4-1 - MobileSync Interface Access Rights

<table>
<thead>
<tr>
<th>Security Reference No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4543</td>
<td>Allow Run Verify Database</td>
</tr>
<tr>
<td>3174</td>
<td>Allow Run Full Sync</td>
</tr>
<tr>
<td>3173</td>
<td>Allow Shut Down MobileSync Application</td>
</tr>
</tbody>
</table>
Appendix A. Parameters

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

**PAR_GROUP MOBILE**

<table>
<thead>
<tr>
<th>PAR Name</th>
<th>PAR Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Crew Card Login Bypass</td>
<td>0 or 1</td>
<td>Allow login using crew card scanning as long as crew credential is valid in Mobile DB.</td>
</tr>
<tr>
<td>Allow to check-in RE/RR person when onboard</td>
<td>0 or 1</td>
<td>Allow to check-in reservation status that is ’RE’/’RE’ when the person is onboard</td>
</tr>
</tbody>
</table>
| 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                                              |
| Require mandatory fields                           | 0 or 1    | 0-Do not require mandatory field  
<p>|                                                   |           | 1-Require mandatory field                                                     |</p>
<table>
<thead>
<tr>
<th>PAR Name</th>
<th>PAR Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Interval</td>
<td>60</td>
<td>Interval time before the next DB synchronization. The default value is 60 seconds.</td>
</tr>
<tr>
<td>Use System Date</td>
<td>0 or 1</td>
<td>0 - Use Device Date 1 - Use System Date</td>
</tr>
</tbody>
</table>

**PAR_GROUP GANGWAY**

Table A-2 - PAR Group Gangway

<table>
<thead>
<tr>
<th>PAR Name</th>
<th>PAR Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow not expected guest to Check-In</td>
<td>0 or 1</td>
<td>0 - Do not allow not expected guest to Check-In 1 - Allow not expected guest to Check-In</td>
</tr>
<tr>
<td>Not allow to check-in Guest if no photo found</td>
<td>0 or 1</td>
<td>0 - Allow guest to check-in without a photo taken 1 - Do not allow guest to check-in if no photo found</td>
</tr>
</tbody>
</table>