Oracle® Hospitality Cruise Shipboard Property Management System

Gangway Security and Mobile Mustering
Installation Guide
Release 7.30.874
E89108-04

September 2018

Contents

Tables

Figures

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

Date	Description of Change
August 2017	▪ Initial publication.
December 2017	▪ Changed method of encryption using a Command Prompt.
May 2018	▪ Log SQL feature were removed
June 2018	▪ Hardcoded passwords/keys were removed
September 2018	▪ Revised .NET Setup

Prerequisites, Supported Systems, and Compatibility

This section describes the minimum requirements for the Application Server for Mobile Mustering 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.

1 System Schematic

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.

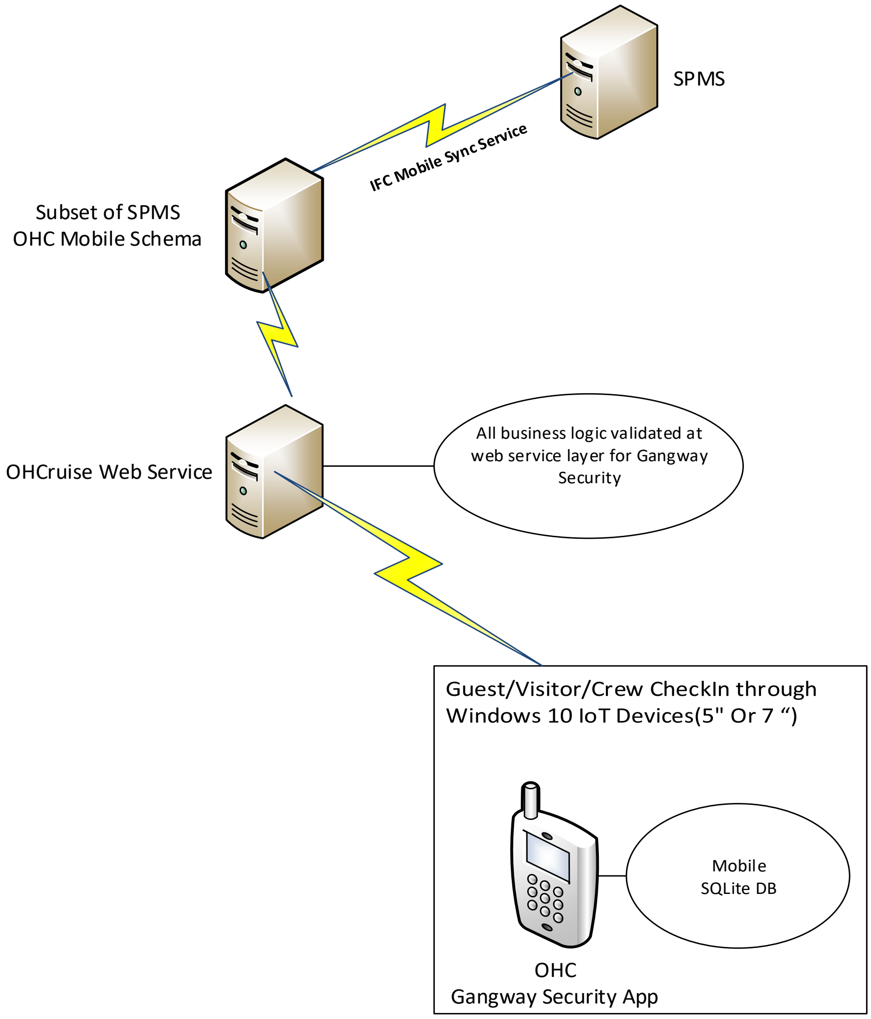

SPMS
IFC Mobile Sync Service
Subset of SPMS
OHC Mobile Schema
OHCruise Web Service
All business logic validated at web service layer for Gangway Security
Guest/Visitor/Crew CheckIn through Windows 10 IoT Devices(5" Or 7 ")
Mobile SQLite DB
OHC
Gangway Security App

Figure 1-1 - Gangway Security System Schematic

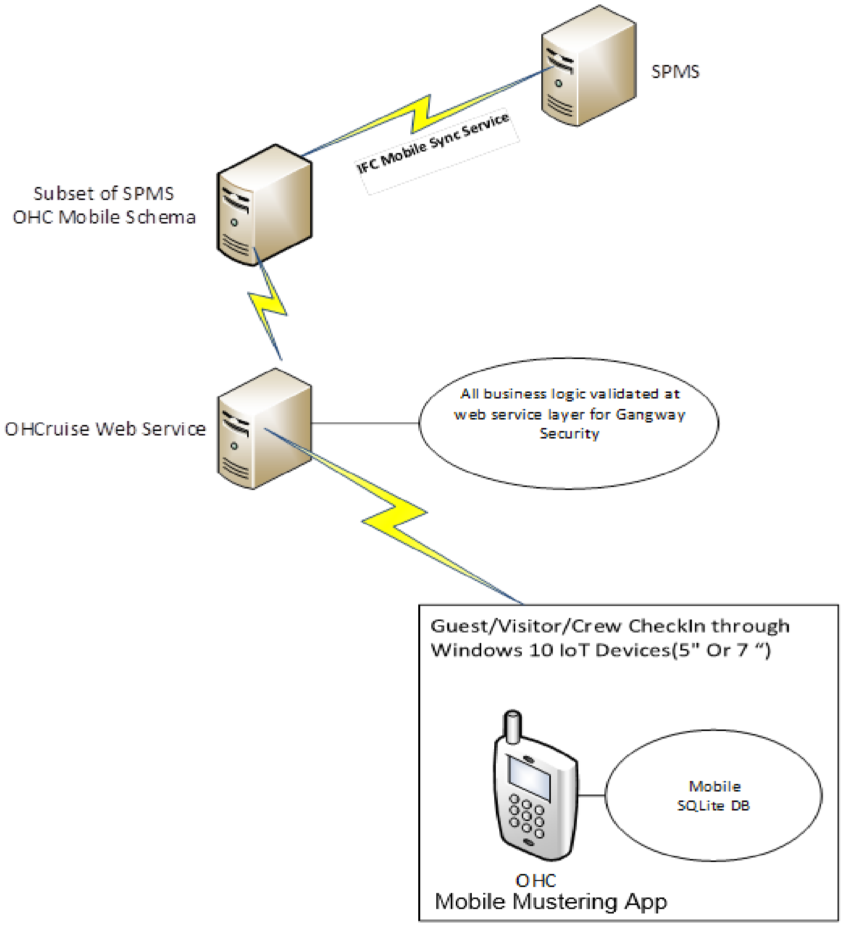

SPMS
IFC Mobile Sync Service
Subset of SPMS
OHC Mobile Schema
OHCruise Web Service
All business logic validated at web service layer for Gangway Security
Guest/Visitor/Crew CheckIn through Windows 10 IoT Devices(5" Or 7 ")
Mobile SQLite DB
OHC
Mobile Mustering App

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.

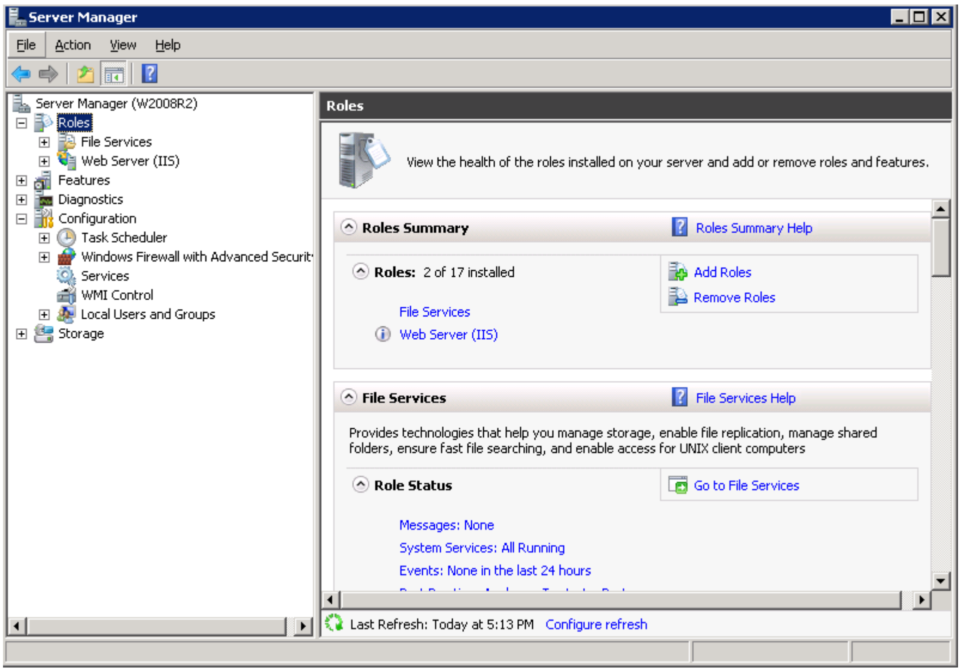
If you do not have a .NET Framework 4.0 installed, download a copy of the installation file from https://www.microsoft.com/en-us/download/developer-tools.aspx and manually run the offline Microsoft .NET Framework 4.0 Installer.

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**.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 2 of 17 installed

File Services

Web Server (IIS)

Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Messages: None

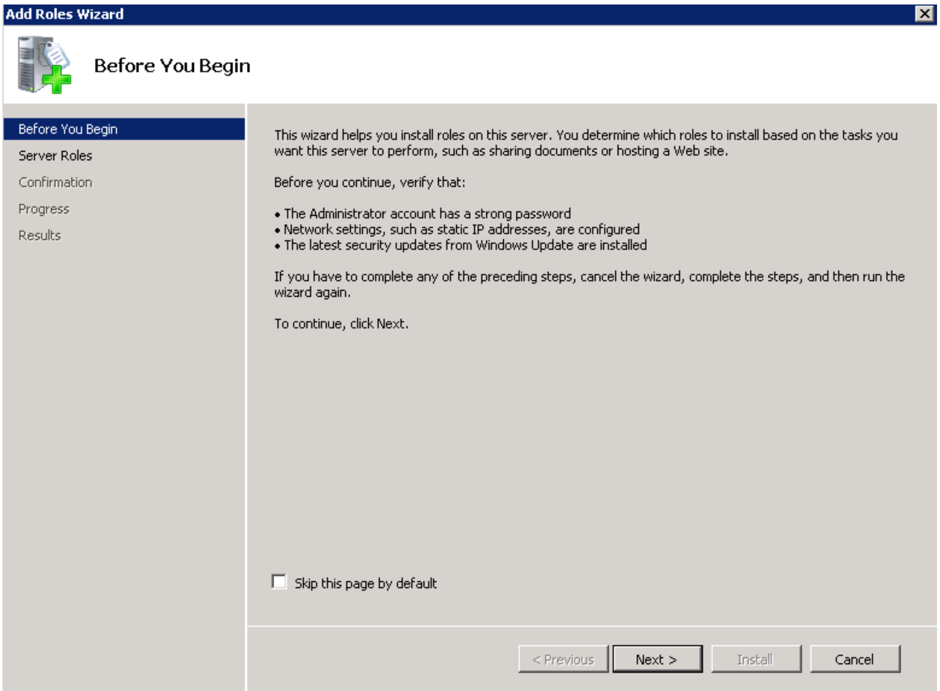
System Services: All Running

Events: None in the last 24 hours

Last Refresh: Today at 5:13 PM

Figure 2-1 – Setting up Mobile Mustering/Gangway Security Server Roles

2. In Before You Begin page, check that the criterion listed on the page are met before continuing.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

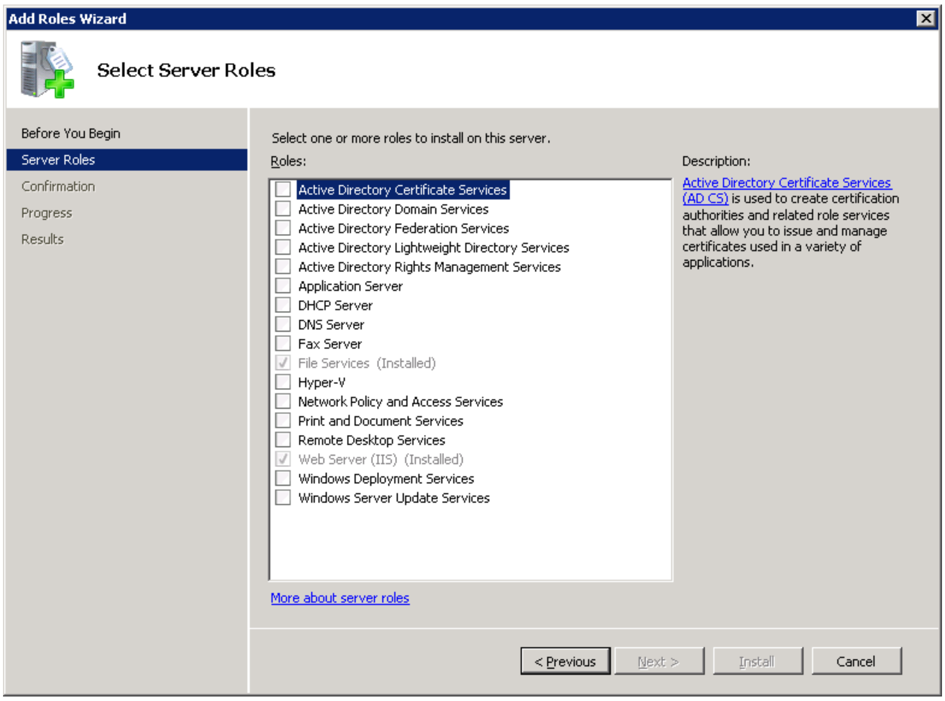
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Figure 2-2 - Adding Server Roles

3. In the Select Server Roles page, select the **File Services and Web Server (IIS)** component check box, and then click **Install**.



Select one or more roles to install on this server.

Roles:

□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server
☑ File Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Desktop Services
☑ Web Server (IIS) (Installed)
□ Windows Deployment Services
□ Windows Server Update Services

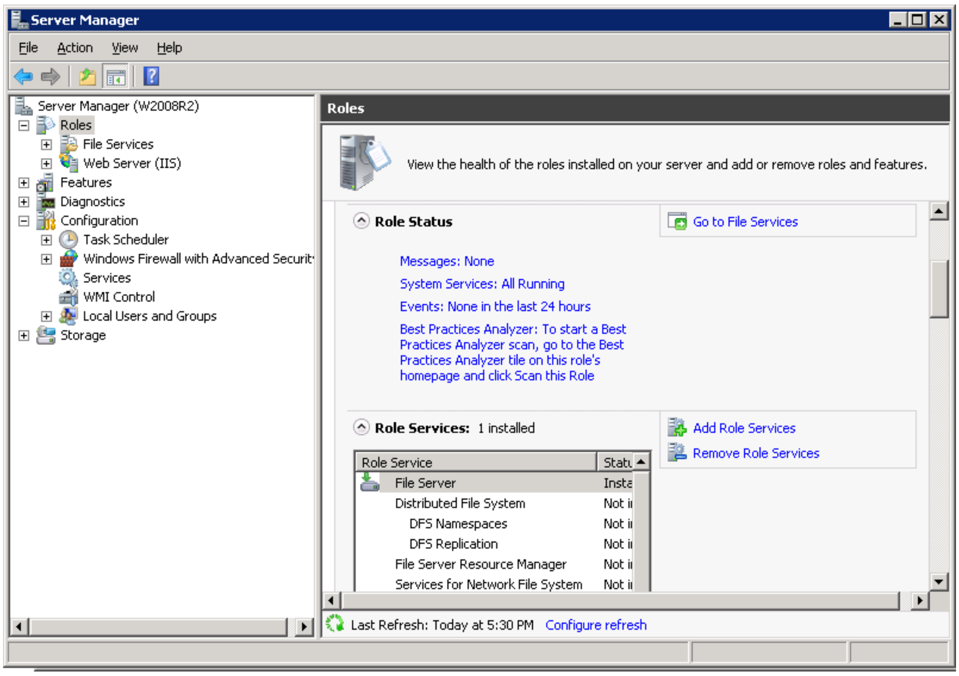
More about server roles

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Figure 2-3 - Server Roles selection in Mobile Mustering App Server

4. At the end of the components installation, select the **Web Server (IIS)** from the Server Manager container, and then select **Add Role Services**.



View the health of the roles installed on your server and add or remove roles and features.

Messages: None
System Services: All Running
Events: None in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

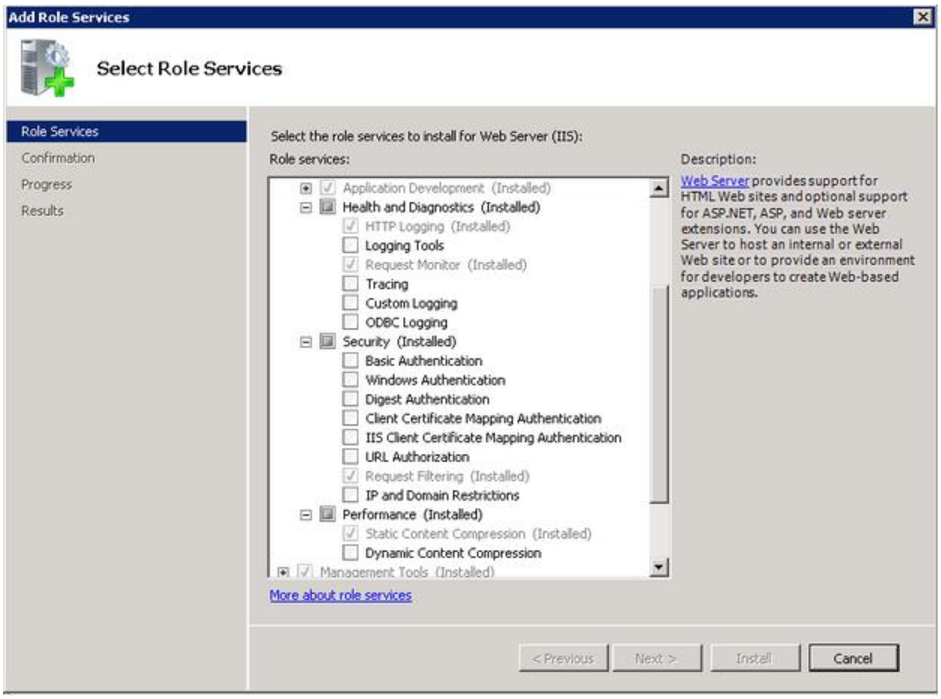
Role Services: 1 installed

Role Service	Statu
File Server	Insta
Distributed File System	Not i
DFS Namespaces	Not i
DFS Replication	Not i
File Server Resource Manager	Not i
Services for Network File System	Not i

Last Refresh: Today at 5:30 PM

Figure 2-4 – Adding WebServices Roles to Mobile App Server

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**.



Select the role services to install for Web Server (IIS):

Role services:

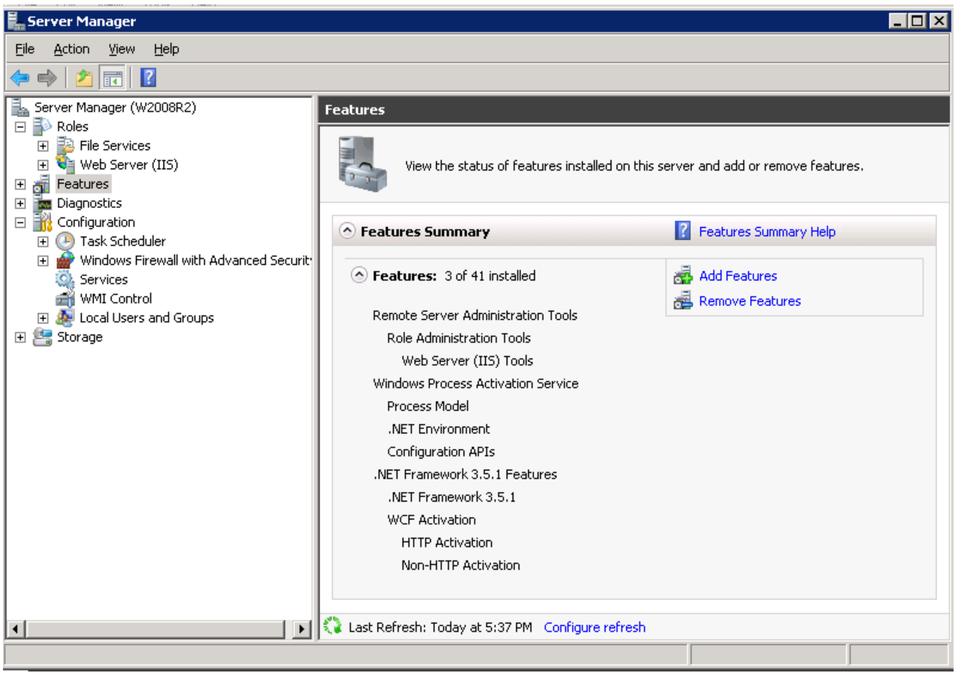
- ☑ Application Development (Installed)
- ☐ Health and Diagnostics (Installed)
  - ☑ HTTP Logging (Installed)
  - ☐ Logging Tools
  - ☑ Request Monitor (Installed)
  - ☐ Tracing
  - ☐ Custom Logging
  - ☐ ODBC Logging
- ☐ Security (Installed)
  - ☐ Basic Authentication
  - ☐ Windows Authentication
  - ☐ Digest Authentication
  - ☐ Client Certificate Mapping Authentication
  - ☐ IIS Client Certificate Mapping Authentication
  - ☐ URL Authorization
  - ☑ Request Filtering (Installed)
  - ☐ IP and Domain Restrictions
- ☐ Performance (Installed)
  - ☑ Static Content Compression (Installed)
  - ☐ Dynamic Content Compression
- ☑ Management Tools (Installed)

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Figure 2-5 - Role Services selection in Mobile App Server

6. Select the **.NET Framework 4.0** and then select **Add Features** from the Server Manager container.



Server Manager (W2008R2)
- Roles
  - File Services
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
  - Task Scheduler
  - Windows Firewall with Advanced Securit
  - Services
  - WMI Control
  - Local Users and Groups
- Storage

View the status of features installed on this server and add or remove features.

Features Summary — Features Summary Help

Features: 3 of 41 installed

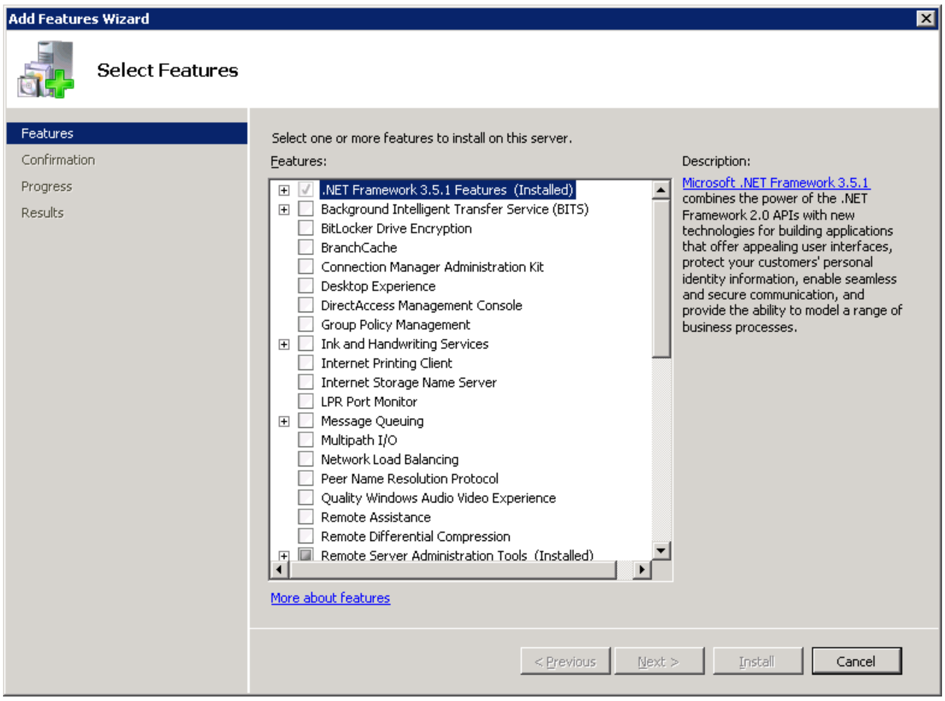
Add Features
Remove Features

Remote Server Administration Tools
Role Administration Tools
Web Server (IIS) Tools
Windows Process Activation Service
Process Model
.NET Environment
Configuration APIs
.NET Framework 3.5.1 Features
.NET Framework 3.5.1
WCF Activation
HTTP Activation
Non-HTTP Activation

Last Refresh: Today at 5:37 PM Configure refresh

Figure 2-6 - Adding Features to Mobile App Server

7. In Select Features screen, select the **.Net Framework 4.0 Features** and **Windows Process Activation Service** check box, and then click **Install**.



Select one or more features to install on this server.

Features:

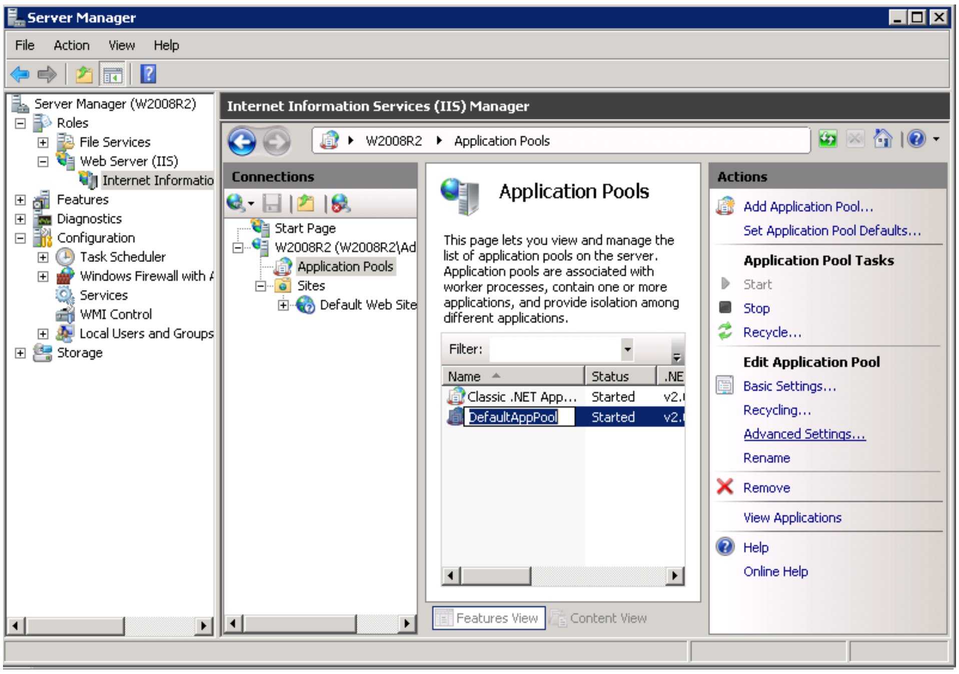
- ☑ .NET Framework 3.5.1 Features (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BranchCache
- ☐ Connection Manager Administration Kit
- ☐ Desktop Experience
- ☐ DirectAccess Management Console
- ☐ Group Policy Management
- ☐ Ink and Handwriting Services
- ☐ Internet Printing Client
- ☐ Internet Storage Name Server
- ☐ LPR Port Monitor
- ☐ Message Queuing
- ☐ Multipath I/O
- ☐ Network Load Balancing
- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ▨ Remote Server Administration Tools (Installed)

Description:

Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 2-7 - Features selection in Mobile Mustering App Server

8. From the Server Manager container, select **Internet Information Services (IIS) Manager**, then **Application Pools, DefaultAppPool,** and then **Advance Settings.**

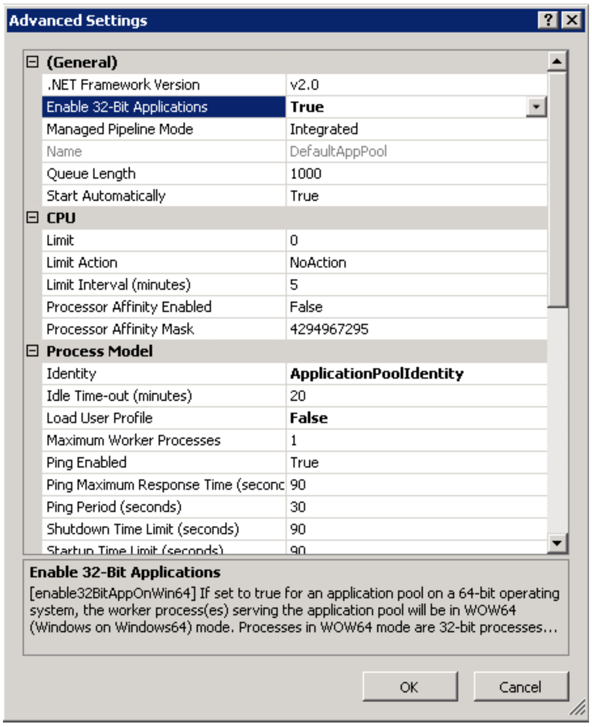


This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NE
Classic .NET App...	Started	v2.(
DefaultAppPool	Started	v2.(

Figure 2-8 - Enabling Advance Settings in IIS

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



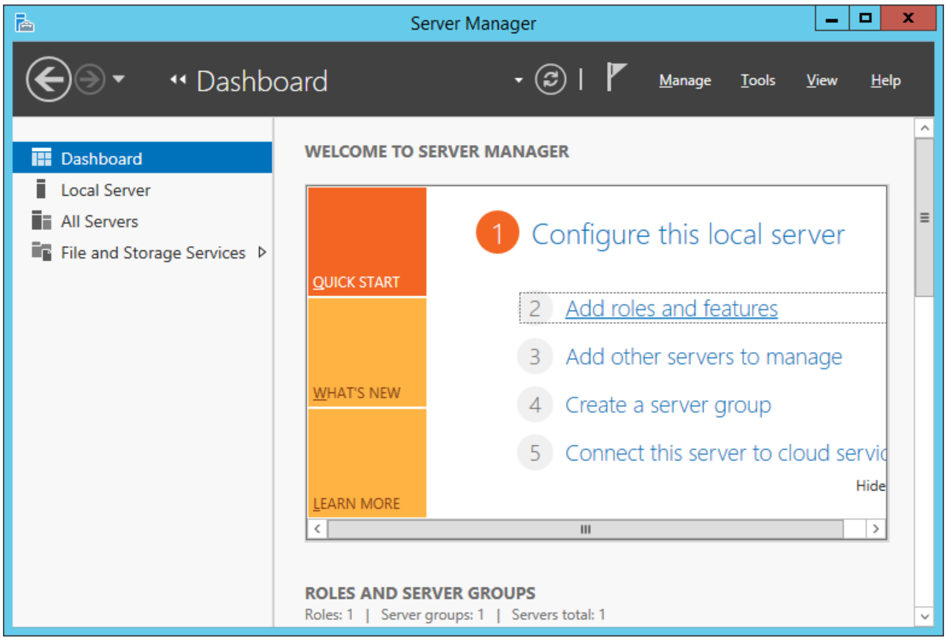
(General)	
.NET Framework Version	v2.0
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Enable 32-Bit Applications
[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mode are 32-bit processes...

Figure 2-9 - IIS Advance Setting

Adding Roles to Microsoft Windows Server 2012 R2

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



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

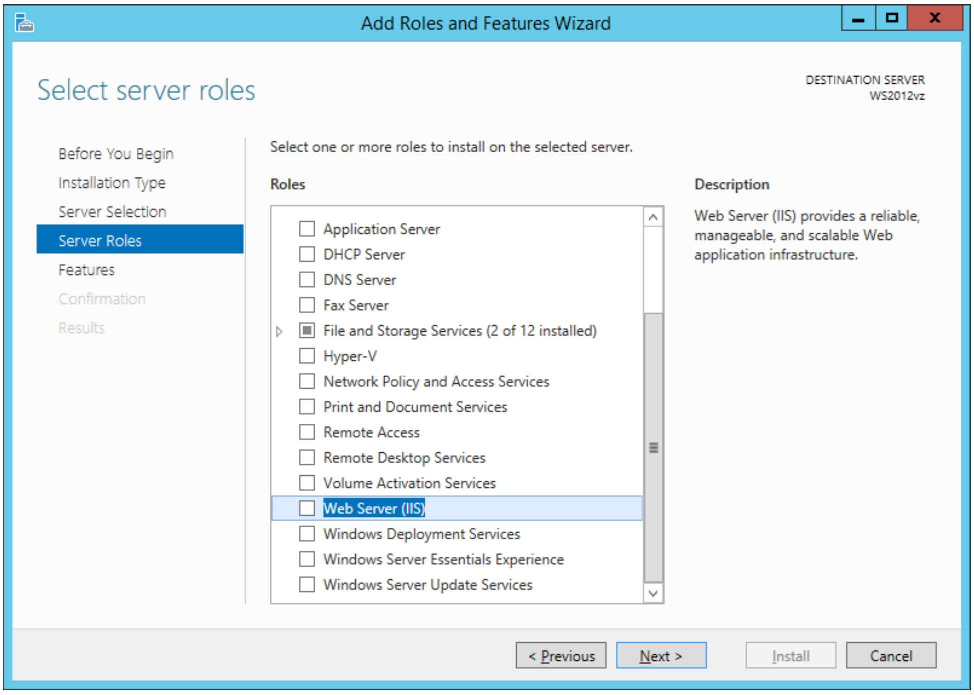
5 Connect this server to cloud servic

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

Figure 2-10 – Mobile Server 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.



Select server roles

DESTINATION SERVER
WS2012vz

Select one or more roles to install on the selected server.

Roles

□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (2 of 12 installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Essentials Experience
□ Windows Server Update Services

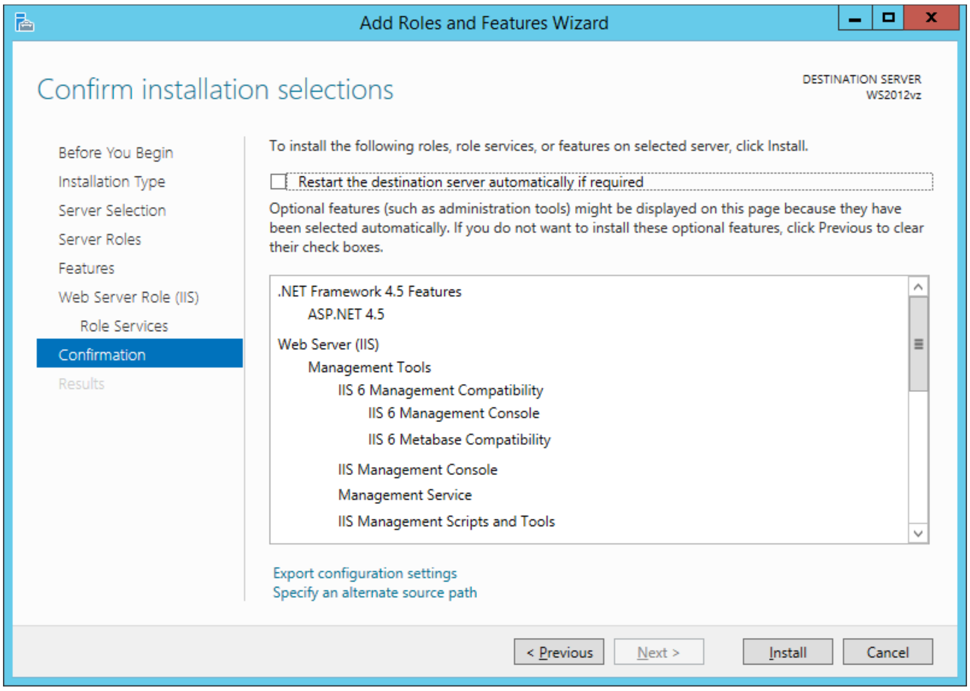
Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 2-11 - Mobile Server Web Server (IIS)

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.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
WS2012vz

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

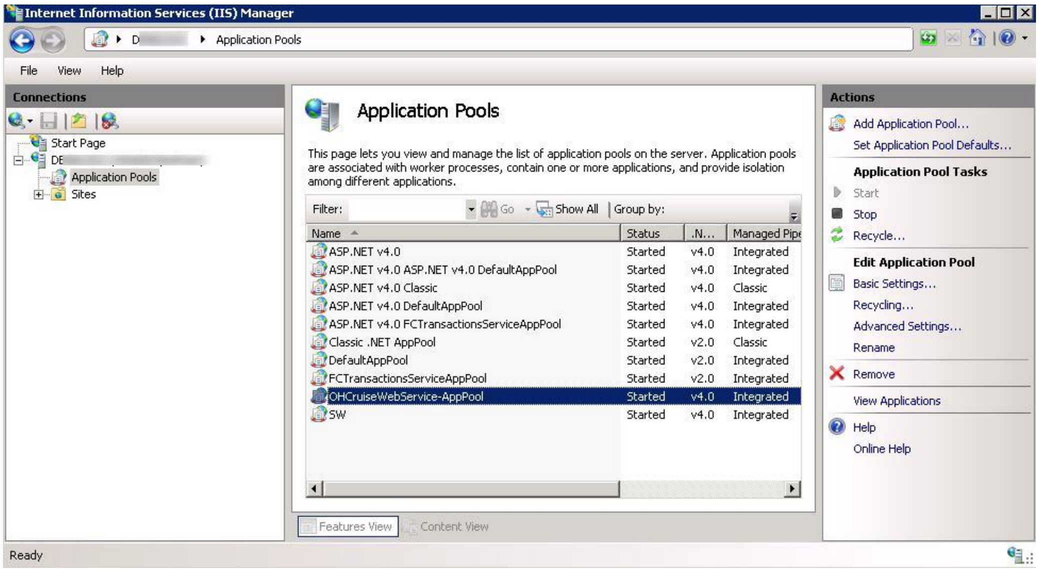
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 4.5 Features
    ASP.NET 4.5
Web Server (IIS)
    Management Tools
        IIS 6 Management Compatibility
            IIS 6 Management Console
            IIS 6 Metabase Compatibility
        IIS Management Console
        Management Service
        IIS Management Scripts and Tools

Export configuration settings
Specify an alternate source path

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**.



Internet Information Services (IIS) Manager

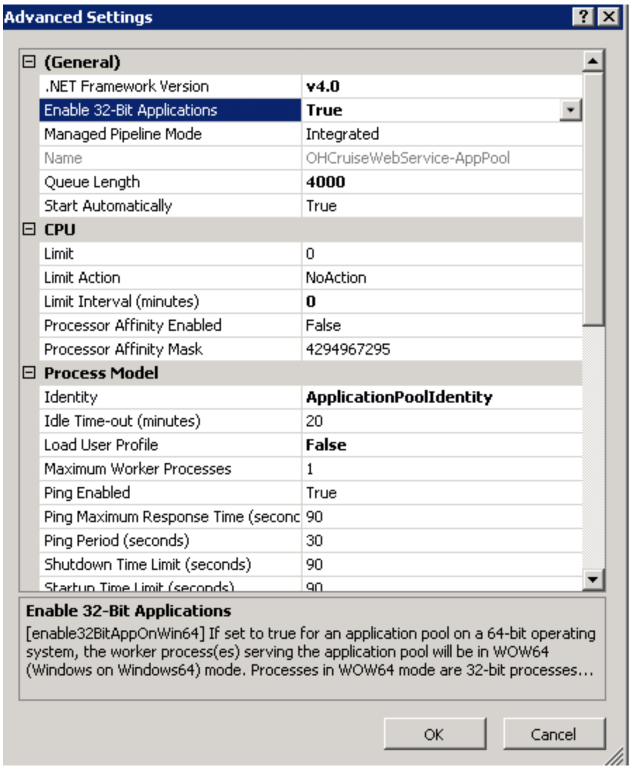
Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.N...	Managed Pipe
ASP.NET v4.0	Started	v4.0	Integrated
ASP.NET v4.0 ASP.NET v4.0 DefaultAppPool	Started	v4.0	Integrated
ASP.NET v4.0 Classic	Started	v4.0	Classic
ASP.NET v4.0 DefaultAppPool	Started	v4.0	Integrated
ASP.NET v4.0 FCTransactionsServiceAppPool	Started	v4.0	Integrated
Classic .NET AppPool	Started	v2.0	Classic
DefaultAppPool	Started	v2.0	Integrated
FCTransactionsServiceAppPool	Started	v2.0	Integrated
OHCruiseWebService-AppPool	Started	v4.0	Integrated
SW	Started	v4.0	Integrated

Figure 2-13 - Enabling Advance Settings in IIS

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



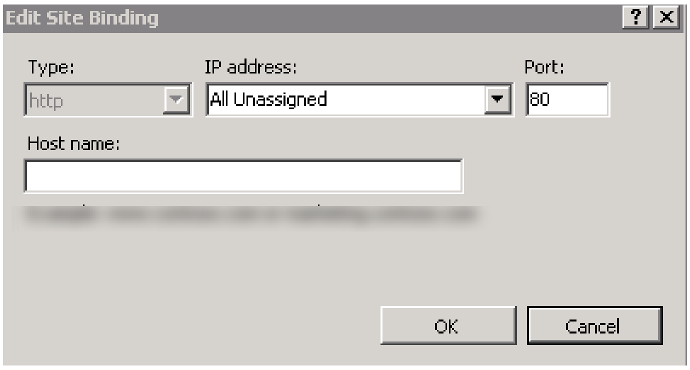
Advanced Settings

(General)	
.NET Framework Version	**v4.0**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	Integrated
Name	OHCruiseWebService-AppPool
Queue Length	**4000**
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	**0**
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Enable 32-Bit Applications
[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mode are 32-bit processes...

Figure 2-14 - IIS Advance Setting

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



Edit Site Binding

Type: http

IP address: All Unassigned

Port: 80

Host name:

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**.

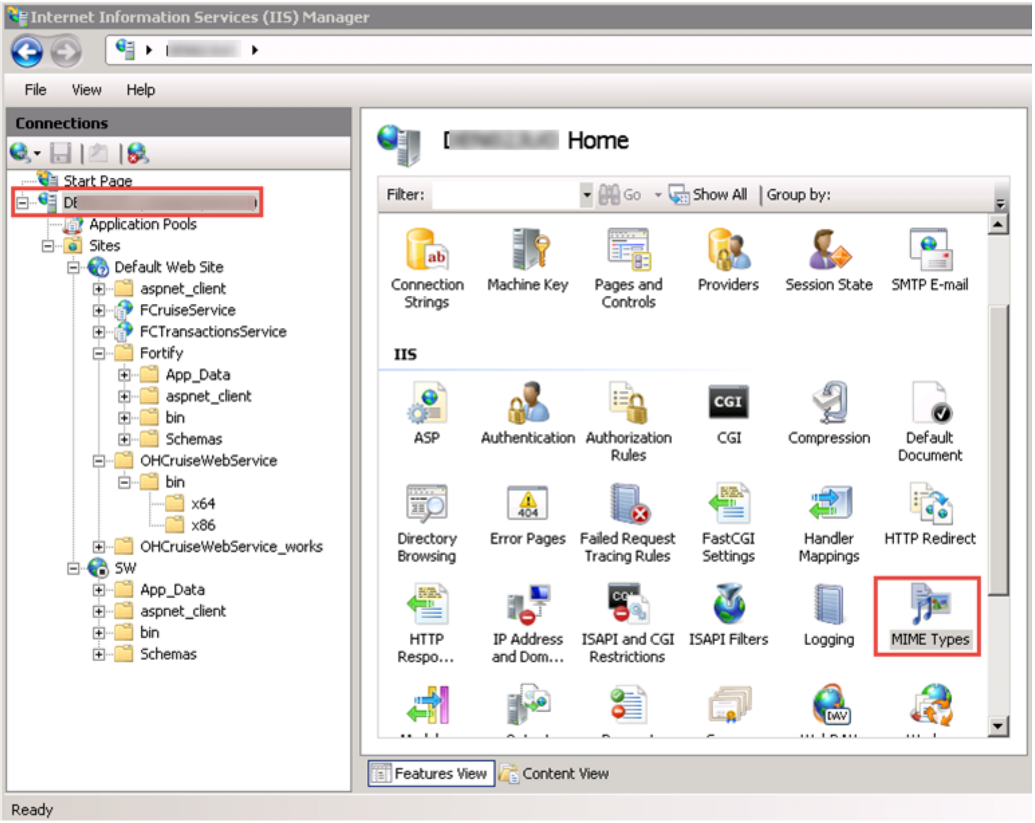


Figure 2-16 - IIS MIME Types

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.

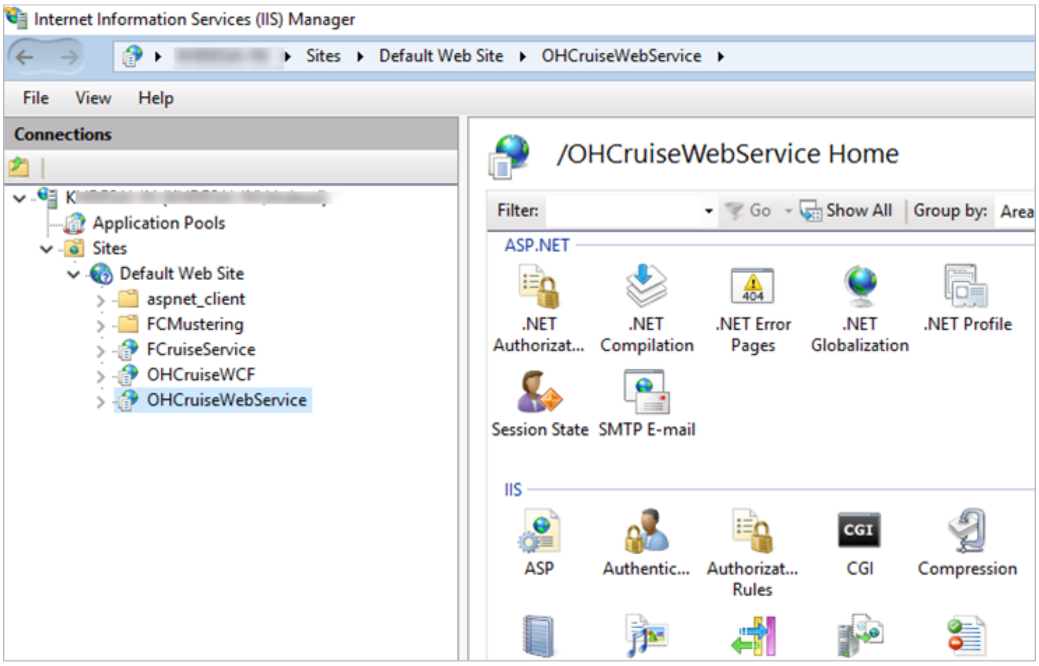
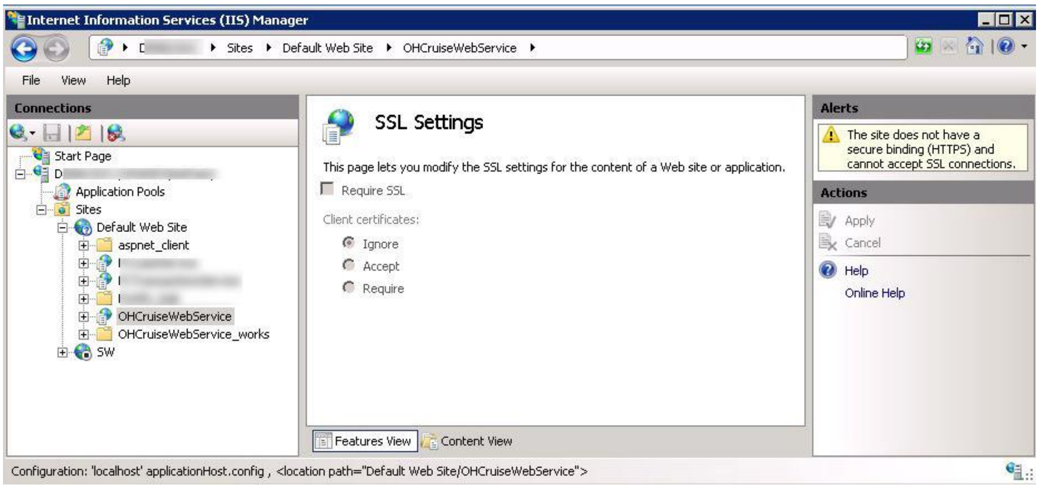


Figure 2-17 - IIS Services

Verifying the Connection without SSL

To ensure that the SSL connection is properly configure,

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 **OHCruiseWebService** and then un-check the **Require SSL** in SSL Settings.



SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

□ Require SSL

Client certificates:

● Ignore

○ Accept

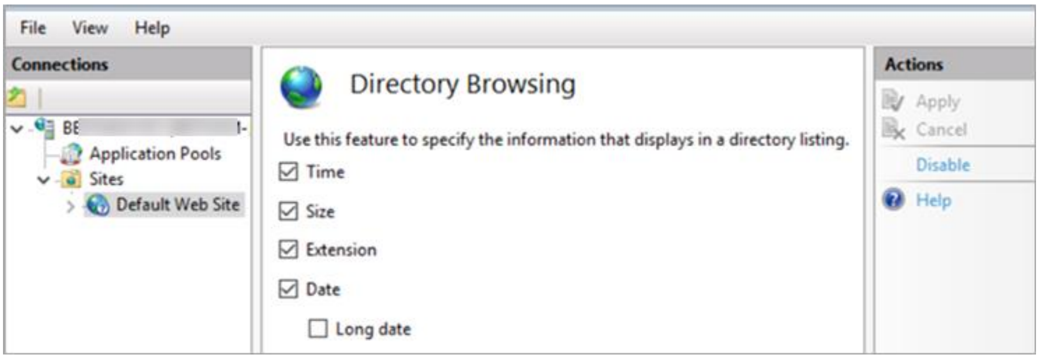
○ Require

The site does not have a secure binding (HTTPS) and cannot accept SSL connections.

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/OHCruiseWebService">

Figure 2-18 - Enabling 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.



Directory Browsing

Use this feature to specify the information that displays in a directory listing.

☑ Time

☑ Size

☑ Extension

☑ Date

□ Long date

Figure 2-19 - Enabling Directory Browsing

5. In the **Default Web Site, OHCruiseWebService**, select **Directory Browsing** and then select **Enable** from the **Actions Panel** on the right.

2.3. Configure OHCruise Web Services

1. Launch the **OHCruiseWebService.msi** application, and then follow installation steps.
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.

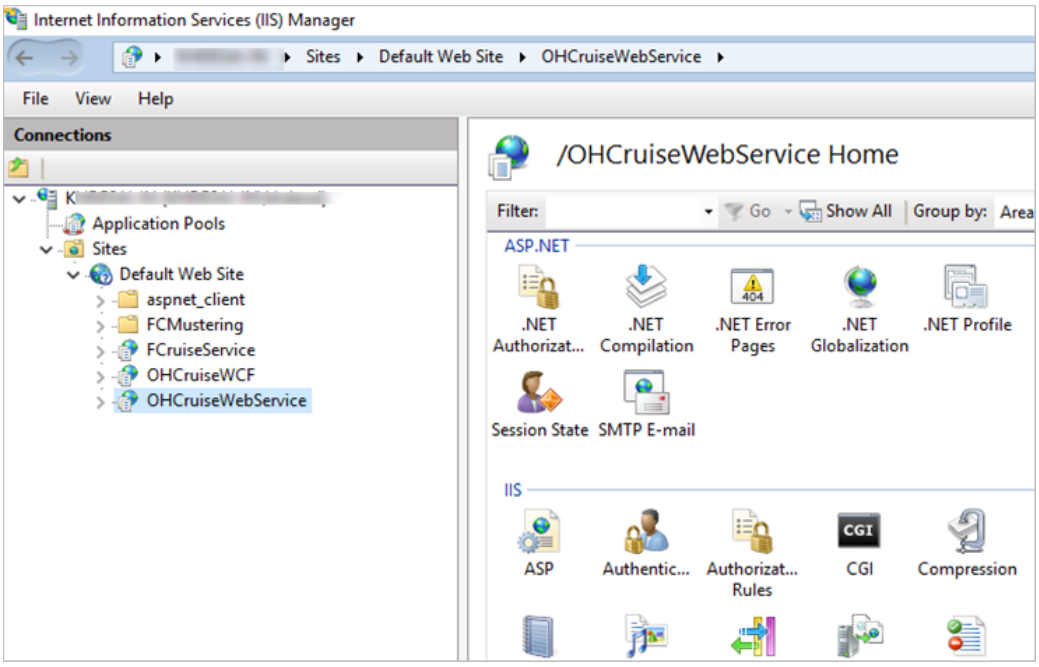


Figure 2-20 - IIS Services

Configuring DB Source for the Web Services

1. From the IIS Manager, Connections section, right-click the **OHCruiseWebService** and select **Explore**. This opens the folder `C:\inetpub\wwwroot\OHCruiseWebService`

2. Locate the **Web.Config** file and edit the following section to point to the correct “Data Source” and then **Save** the file.

```
<connectionStrings
configProtectionProvider="RsaProtectedConfigurationProvide
r">
<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.

```
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.

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:

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

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

Decrypting 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.

aspnet_regiis -pdf "connectionStrings" C:\Projects\OHCruiseWebService

Verifying the WebServices connection

To ensure the WebServices connection is properly setup,

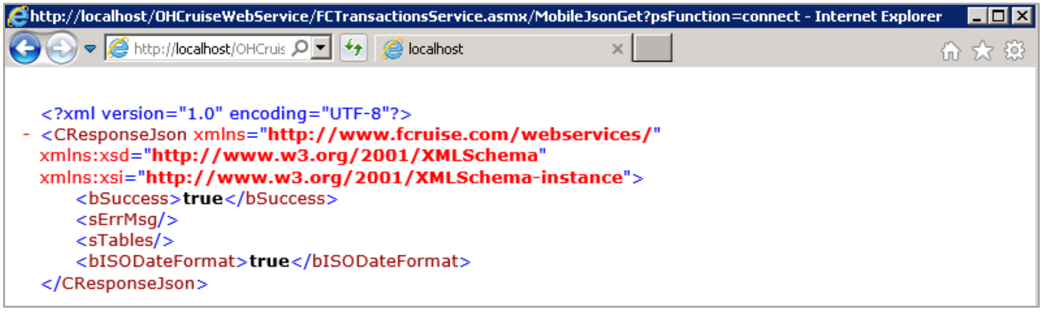
1. Open the web browser of the machine where the web service is installed.
2. Copy and paste the following URL into your browser.

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

   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.



http://localhost/OHCruiseWebService/FCTransactionsService.asmx/MobileJsonGet?psFunction=connect - Internet Explorer
http://localhost/OHCruis
localhost

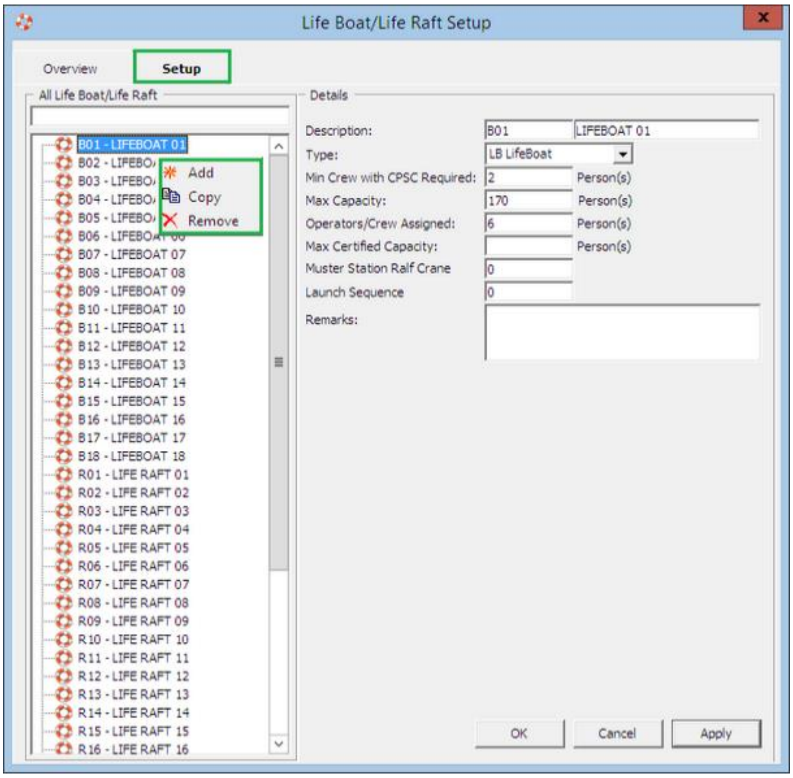
```
  <?xml version="1.0" encoding="UTF-8"?>
- <CResponseJson xmlns="http://www.fcruise.com/webservices/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <bSuccess>true</bSuccess>
      <sErrMsg/>
      <sTables/>
      <bISODateFormat>true</bISODateFormat>
  </CResponseJson>
```

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

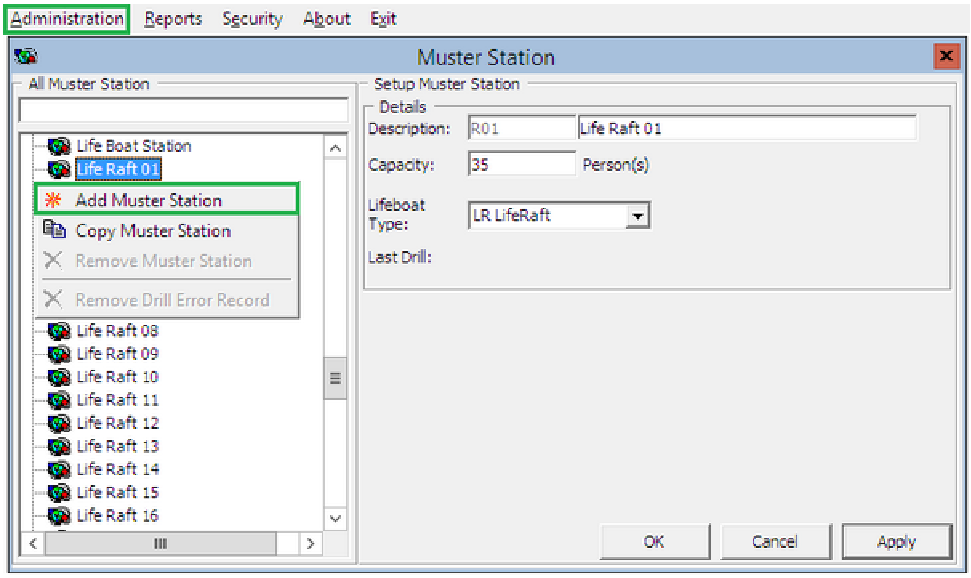


Description: B01 LIFEBOAT 01
Type: LB LifeBoat
Min Crew with CPSC Required: 2 Person(s)
Max Capacity: 170 Person(s)
Operators/Crew Assigned: 6 Person(s)
Max Certified Capacity: Person(s)
Muster Station Ralf Crane 0
Launch Sequence 0
Remarks:

Figure 2-22 - Adding Lifeboat/LifeRaft

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



Setup Muster Station

Details

Description: R01 Life Raft 01

Capacity: 35 Person(s)

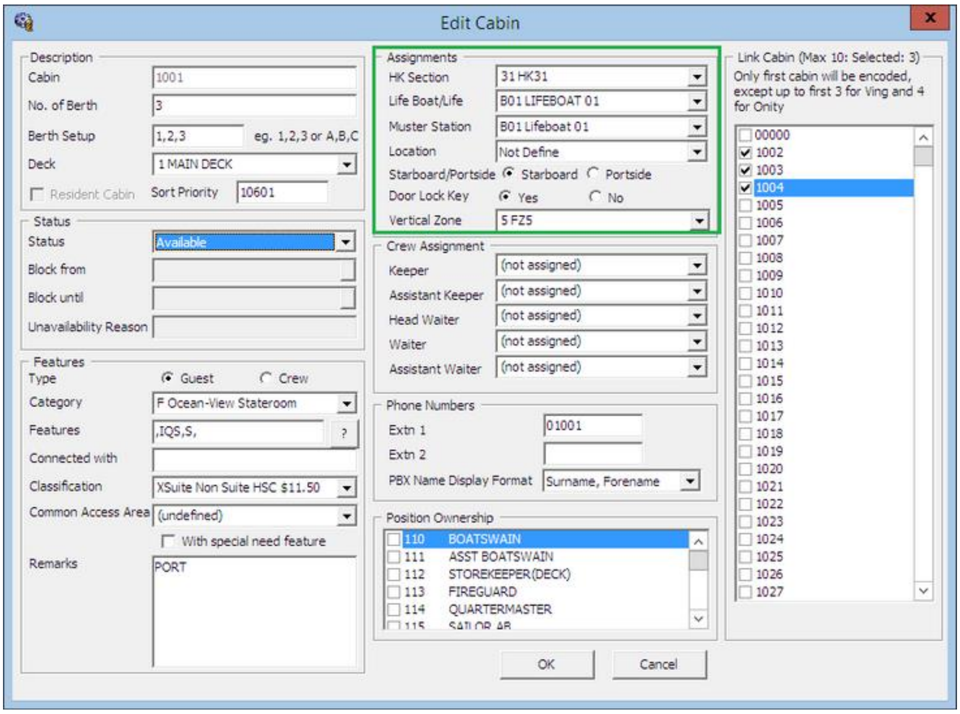
Lifeboat Type: LR LifeRaft

Last Drill:

Figure 2-23 - Adding Muster Station

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



Description

Cabin: 1001

No. of Berth: 3

Berth Setup: 1,2,3 eg. 1,2,3 or A,B,C

Deck: 1 MAIN DECK

□ Resident Cabin Sort Priority: 10601

Status

Status: Available

Block from:

Block until:

Unavailability Reason:

Features

Type: ● Guest ○ Crew

Category: F Ocean-View Stateroom

Features: ,IQS,S, ?

Connected with:

Classification: XSuite Non Suite HSC $11.50

Common Access Area: (undefined)

□ With special need feature

Remarks: PORT

Assignments

HK Section: 31 HK31

Life Boat/Life: B01 LIFEBOAT 01

Muster Station: B01 Lifeboat 01

Location: Not Define

Starboard/Portside: ● Starboard ○ Portside

Door Lock Key: ● Yes ○ No

Vertical Zone: 5 FZ5

Crew Assignment

Keeper: (not assigned)

Assistant Keeper: (not assigned)

Head Waiter: (not assigned)

Waiter: (not assigned)

Assistant Waiter: (not assigned)

Phone Numbers

Extn 1: 01001

Extn 2:

PBX Name Display Format: Surname, Forename

Position Ownership

□ 110 BOATSWAIN
□ 111 ASST BOATSWAIN
□ 112 STOREKEEPER(DECK)
□ 113 FIREGUARD
□ 114 QUARTERMASTER
□ 115 SAILOR AB

Link Cabin (Max 10: Selected: 3)

Only first cabin will be encoded, except up to first 3 for Ving and 4 for Onity

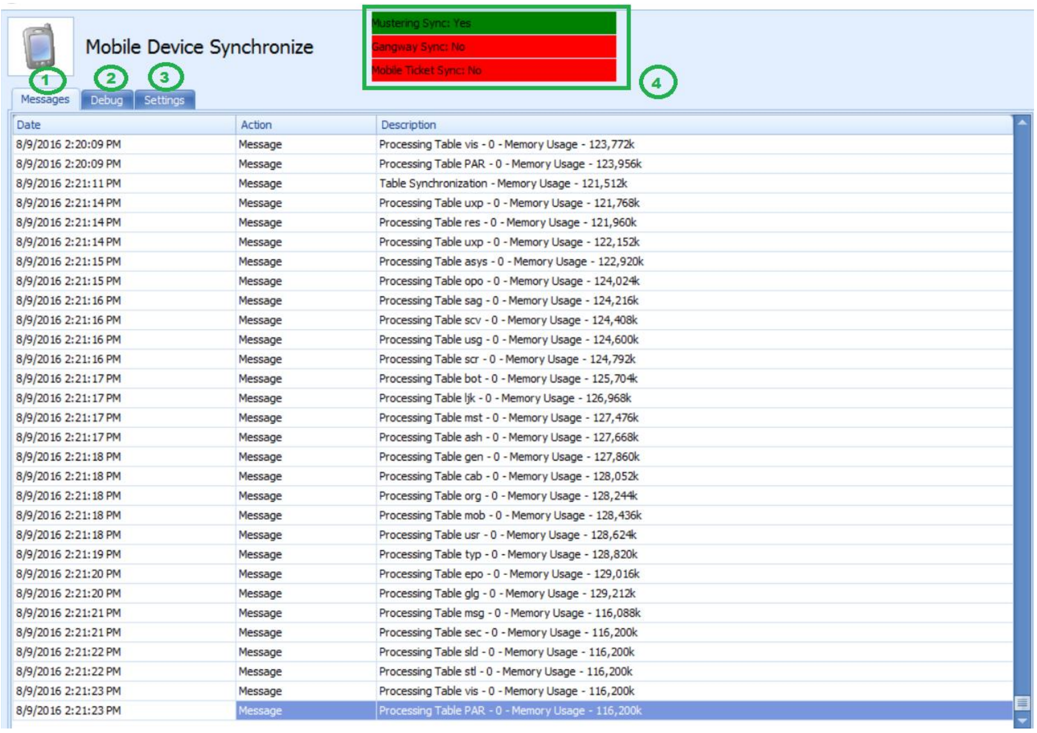
□ 00000
☑ 1002
☑ 1003
☑ 1004
□ 1005
□ 1006
□ 1007
□ 1008
□ 1009
□ 1010
□ 1011
□ 1012
□ 1013
□ 1014
□ 1015
□ 1016
□ 1017
□ 1018
□ 1019
□ 1020
□ 1021
□ 1022
□ 1023
□ 1024
□ 1025
□ 1026
□ 1027

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**.



Mustering Sync: Yes
Gangway Sync: No
Mobile Ticket Sync: No

Date	Action	Description
8/9/2016 2:20:09 PM	Message	Processing Table vis - 0 - Memory Usage - 123,772k
8/9/2016 2:20:09 PM	Message	Processing Table PAR - 0 - Memory Usage - 123,956k
8/9/2016 2:21:11 PM	Message	Table Synchronization - Memory Usage - 121,512k
8/9/2016 2:21:14 PM	Message	Processing Table uxp - 0 - Memory Usage - 121,768k
8/9/2016 2:21:14 PM	Message	Processing Table res - 0 - Memory Usage - 121,960k
8/9/2016 2:21:14 PM	Message	Processing Table uxp - 0 - Memory Usage - 122,152k
8/9/2016 2:21:15 PM	Message	Processing Table asys - 0 - Memory Usage - 122,920k
8/9/2016 2:21:15 PM	Message	Processing Table opo - 0 - Memory Usage - 124,024k
8/9/2016 2:21:16 PM	Message	Processing Table sag - 0 - Memory Usage - 124,216k
8/9/2016 2:21:16 PM	Message	Processing Table scv - 0 - Memory Usage - 124,408k
8/9/2016 2:21:16 PM	Message	Processing Table usg - 0 - Memory Usage - 124,600k
8/9/2016 2:21:16 PM	Message	Processing Table scr - 0 - Memory Usage - 124,792k
8/9/2016 2:21:17 PM	Message	Processing Table bot - 0 - Memory Usage - 125,704k
8/9/2016 2:21:17 PM	Message	Processing Table ljk - 0 - Memory Usage - 126,968k
8/9/2016 2:21:17 PM	Message	Processing Table mst - 0 - Memory Usage - 127,476k
8/9/2016 2:21:17 PM	Message	Processing Table ash - 0 - Memory Usage - 127,668k
8/9/2016 2:21:18 PM	Message	Processing Table gen - 0 - Memory Usage - 127,860k
8/9/2016 2:21:18 PM	Message	Processing Table cab - 0 - Memory Usage - 128,052k
8/9/2016 2:21:18 PM	Message	Processing Table org - 0 - Memory Usage - 128,244k
8/9/2016 2:21:18 PM	Message	Processing Table mob - 0 - Memory Usage - 128,436k
8/9/2016 2:21:18 PM	Message	Processing Table usr - 0 - Memory Usage - 128,624k
8/9/2016 2:21:19 PM	Message	Processing Table typ - 0 - Memory Usage - 128,820k
8/9/2016 2:21:20 PM	Message	Processing Table epo - 0 - Memory Usage - 129,016k
8/9/2016 2:21:20 PM	Message	Processing Table glg - 0 - Memory Usage - 129,212k
8/9/2016 2:21:21 PM	Message	Processing Table msg - 0 - Memory Usage - 116,088k
8/9/2016 2:21:21 PM	Message	Processing Table sec - 0 - Memory Usage - 116,200k
8/9/2016 2:21:22 PM	Message	Processing Table sld - 0 - Memory Usage - 116,200k
8/9/2016 2:21:22 PM	Message	Processing Table stl - 0 - Memory Usage - 116,200k
8/9/2016 2:21:23 PM	Message	Processing Table vis - 0 - Memory Usage - 116,200k
8/9/2016 2:21:23 PM	Message	Processing Table PAR - 0 - Memory Usage - 116,200k

Figure 2-25 - IFC MobileSync Interface screen

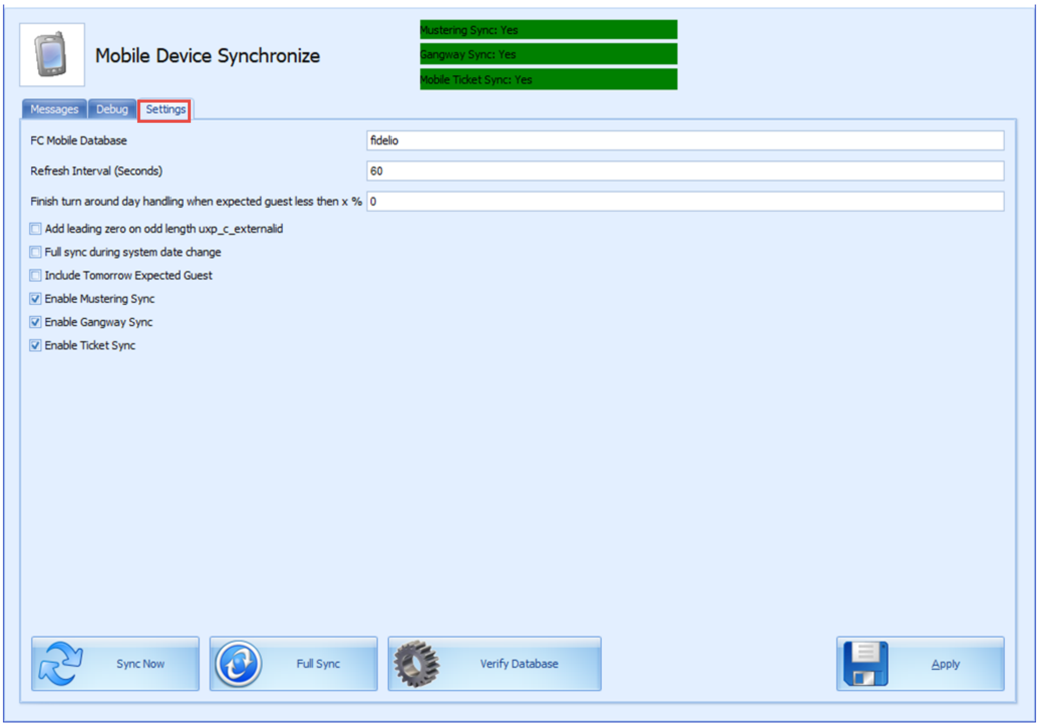
Table 2-1 - Function definition of IFC MobileSync

Field Name	Field Definitions
1.	Tab indicates all synchronization activities.
2.	Tab represents all activities in debugging format with SQL Command.
3.	Tab defines the required settings and synchronization functions.
4.	Labels that define the types of synchronization enabled from the Settings tab.

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.



Mustering Sync: Yes

Gangway Sync: Yes

Mobile Ticket Sync: Yes

FC Mobile Database: fidelio

Refresh Interval (Seconds): 60

Finish turn around day handling when expected guest less then x %: 0

☐ Add leading zero on odd length uxp_c_externalid

☐ Full sync during system date change

☐ Include Tomorrow Expected Guest

☑ Enable Mustering Sync

☑ Enable Gangway Sync

☑ Enable Ticket Sync

Figure 2-26 - OHC MobileSync Settings

Below are the Optional functions available in OHC MobileSync Settings:

Table 2-2 - Field definition of OHC MobileSync Settings

Field Name	Field Definitions
Refresh Interval (Seconds)	Triggers synchronization automatically according to the pre-defined seconds. The default is 60seconds.
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.

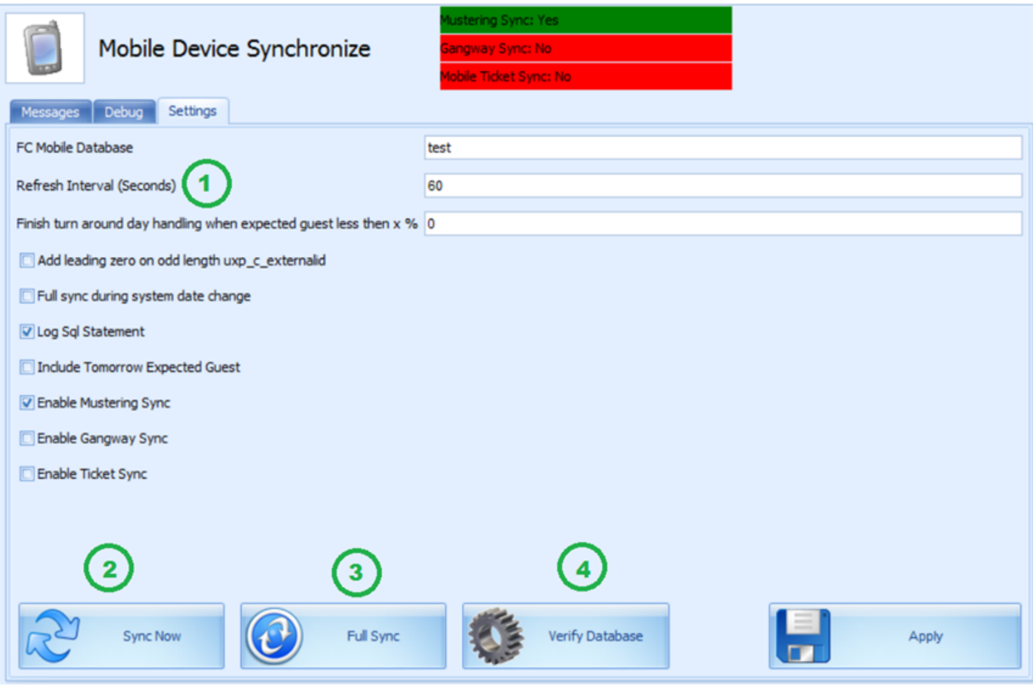
Field Name	Field Definitions
Add leading zero on odd length uxp_c_externalid	This function adds leading zero to the UXP_C_EXTERNALID (Odd length) in FCMOBILE DB whenever a full synchronization is performed.
Full Sync during system date change	This function automatically triggers a Full Synchronization 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 prior to updating it with the latest data from 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

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.



Mobile Device Synchronize

Mustering Sync: Yes
Gangway Sync: No
Mobile Ticket Sync: No

FC Mobile Database: test
Refresh Interval (Seconds): 60
Finish turn around day handling when expected guest less then x %: 0

☐ Add leading zero on odd length uxp_c_externalid
☐ Full sync during system date change
☑ Log Sql Statement
☐ Include Tomorrow Expected Guest
☑ Enable Mustering Sync
☐ Enable Gangway Sync
☐ Enable Ticket Sync

Figure 2-27 - OHC MobileSync Settings page

Performing a Synchronization

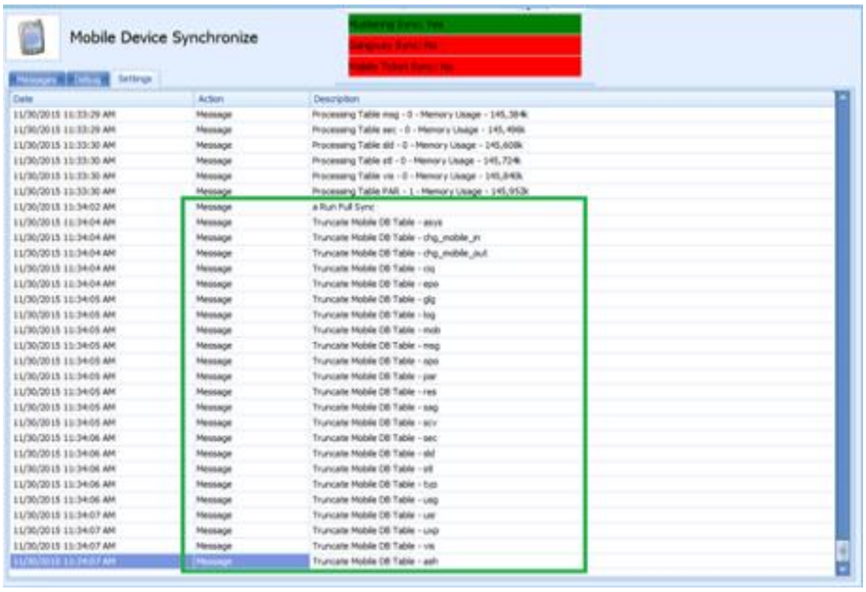
1. At the **Settings** tab of MobileSync application, verify that the **FC Mobile Database** is pointing to the correct ship database[1]. If not, correct the database name and click **Apply** to save the changes.
2. Select **Sync Now**[2] to perform the synchronization immediately.
3. If the parameter `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**[3] 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.



Date	Action	Description
11/30/2015 11:33:29 AM	Message	Processing Table msg - 0 - Memory Usage - 145,384k
11/30/2015 11:33:29 AM	Message	Processing Table sec - 0 - Memory Usage - 145,496k
11/30/2015 11:33:30 AM	Message	Processing Table sld - 0 - Memory Usage - 145,608k
11/30/2015 11:33:30 AM	Message	Processing Table stl - 0 - Memory Usage - 145,724k
11/30/2015 11:33:30 AM	Message	Processing Table vis - 0 - Memory Usage - 145,840k
11/30/2015 11:33:30 AM	Message	Processing Table PAR - 1 - Memory Usage - 145,952k
11/30/2015 11:34:02 AM	Message	a Run Full Sync
11/30/2015 11:34:04 AM	Message	Truncate Mobile DB Table - asys
11/30/2015 11:34:04 AM	Message	Truncate Mobile DB Table - chg_mobile_in
11/30/2015 11:34:04 AM	Message	Truncate Mobile DB Table - chg_mobile_out
11/30/2015 11:34:04 AM	Message	Truncate Mobile DB Table - cig
11/30/2015 11:34:04 AM	Message	Truncate Mobile DB Table - epo
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - glg
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - log
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - mob
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - msg
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - opo
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - par
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - res
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - sag
11/30/2015 11:34:05 AM	Message	Truncate Mobile DB Table - scv
11/30/2015 11:34:06 AM	Message	Truncate Mobile DB Table - sec
11/30/2015 11:34:06 AM	Message	Truncate Mobile DB Table - sld
11/30/2015 11:34:06 AM	Message	Truncate Mobile DB Table - stl
11/30/2015 11:34:06 AM	Message	Truncate Mobile DB Table - tco
11/30/2015 11:34:06 AM	Message	Truncate Mobile DB Table - usg
11/30/2015 11:34:07 AM	Message	Truncate Mobile DB Table - usr
11/30/2015 11:34:07 AM	Message	Truncate Mobile DB Table - usp
11/30/2015 11:34:07 AM	Message	Truncate Mobile DB Table - vis
11/30/2015 11:34:07 AM	Message	Truncate Mobile DB Table - ash

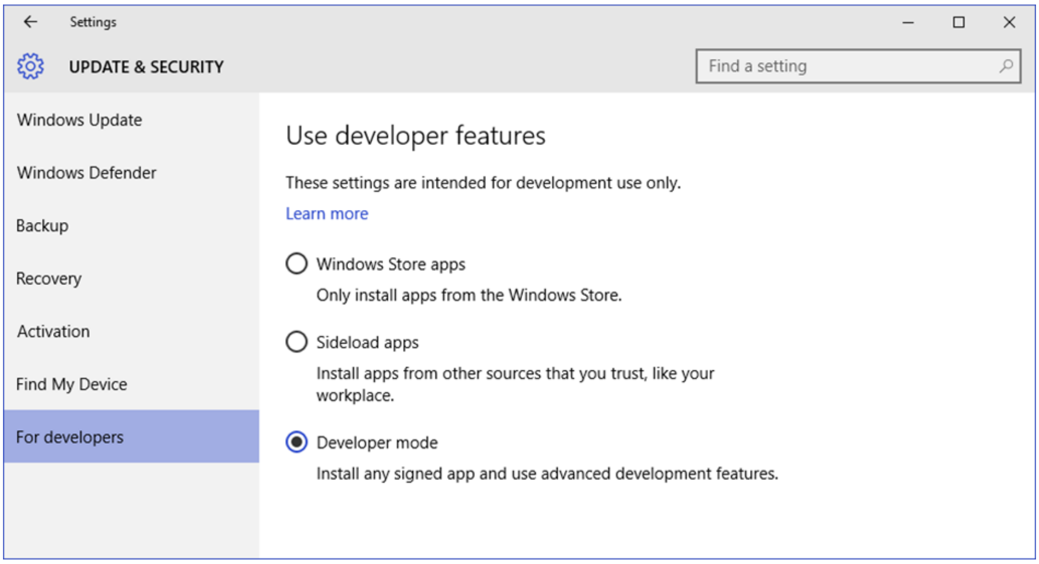
Figure 2-28 – Synchronized tables in OHC MobileSync

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 Mustering and Gangway Security application would require the Developer Mode of the mobile device to be turned on.



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

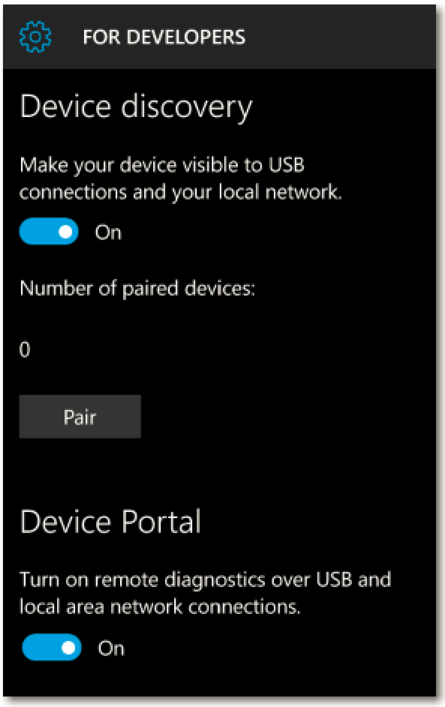
1. Press the **Windows + I** keys simultaneously on the mobile device to open the **Settings** window.
2. Select **Update & Security.**
3. On the left of the screen, click **For Developers**.
4. Under "Use developer features" select the **Developer mode** option.
5. Restart the computer/mobile device.

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.



FOR DEVELOPERS

Device discovery

Make your device visible to USB connections and your local network.

On

Number of paired devices:

0

Pair

Device Portal

Turn on remote diagnostics over USB and local area network connections.

On

Figure 3-2 - Turn On Device Discovery

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.

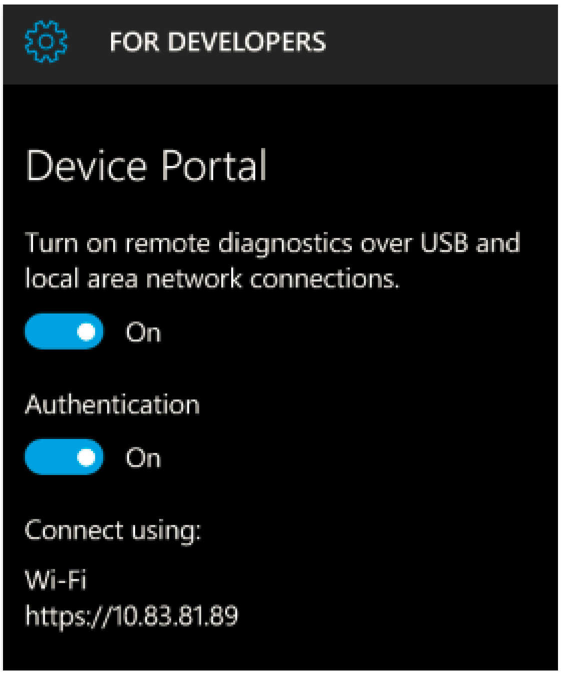
- **USB:** `http://127.0.0.1:10080`

  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>`

  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. This is useful for devices that change their networks or IP addresses frequently, or need to be shared.



FOR DEVELOPERS

Device Portal

Turn on remote diagnostics over USB and local area network connections.

On

Authentication

On

Connect using:

Wi-Fi
https://10.83.81.89

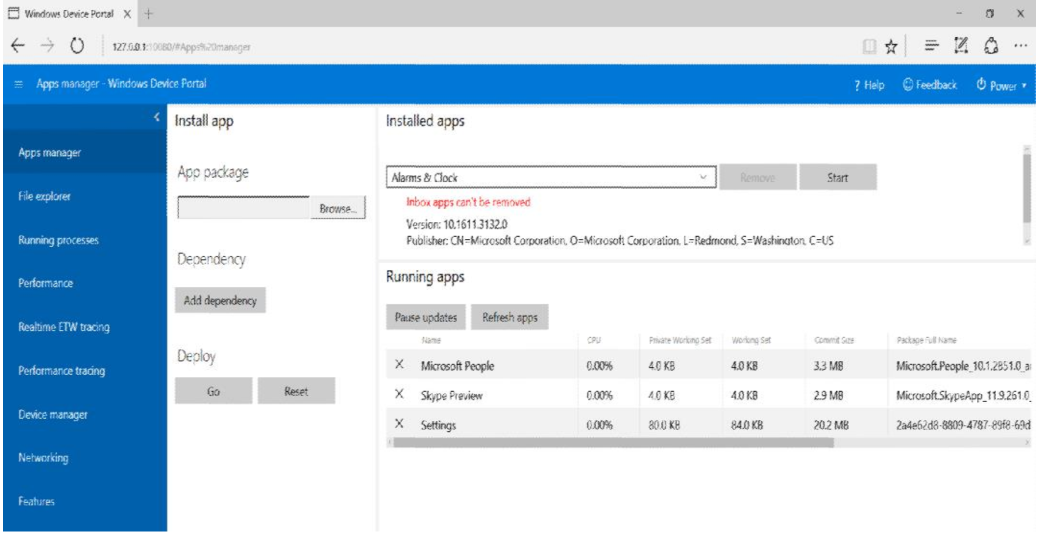
Figure 3-3 - Connect Using

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.



Install app

App package

Dependency

Deploy

Installed apps

Alarms & Clock

Inbox apps can't be removed

Version: 10.1611.3132.0
Publisher: CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

Running apps

	Name	CPU	Private Working Set	Working Set	Commit Size	Package Full Name
X	Microsoft People	0.00%	4.0 KB	4.0 KB	3.3 MB	Microsoft.People_10.1.2851.0_a
X	Skype Preview	0.00%	4.0 KB	4.0 KB	2.9 MB	Microsoft.SkypeApp_11.9.261.0_
X	Settings	0.00%	80.0 KB	84.0 KB	20.2 MB	2a4e62d8-8809-4787-89f8-69d

Figure 3-4 - Windows Device Portal

- **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**.

4 User Security Group

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

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

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 A-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
Require mandatory fields	0 or 1	0-Do not require mandatory field 1-Require mandatory field

PAR Name	PAR Value	Description
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

PAR_GROUP GANGWAY

Table A-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