

Oracle® Hospitality Cruise Fleet Management

Installation and Upgrade Guide



Release 9.1
F13419-10
August 2022

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

ORACLE®

Copyright © 2004, 2022, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

Preface

1 Prerequisites

Database Server	1-1
Internet Information Services (IIS) Web Server	1-1
FMS Application Client	1-2
Network	1-2

2 Pre-Installation Task

Microsoft .Net Framework Version	2-1
----------------------------------	-----

3 Uninstalling Fleet Management Component or Add Ons

4 IIS Web Server Configuration

5 Installation of Fleet Management Component or Add-On

Installation Notes	5-1
Post Installation Notes	5-2

6 Performing FMS Upgrade

What You Should Know	6-1
Before You Begin	6-1
Acquiring the patches	6-1
Installing the patches	6-2
Installing a New Application for Sender and Receiver Services	6-2
Updating Sender/Receiver	6-6
Upgrading to FMS 9.1	6-7

FMS Upgrade Plan	6-9
Step 1	6-10
Step 2	6-12
Step 3	6-13
Step 4	6-14
Step 5	6-15
Step 6	6-16
Step 7	6-17
Step 8	6-18
Step 9	6-19

Preface

This document describes the installation process of Fleet Management Components or Add-Ons.

Audience

This document is intended for the technical personnel involved in installation process of the Fleet Management Components or Add-Ons.

Customer Support

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

<https://support.oracle.com>.

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

Date	Description of Change
August 2019	<ul style="list-style-type: none">• Initial publication.
August 2019	<ul style="list-style-type: none">• Republished PDF formatted version to include Chapter 7 FMS Upgrade Plan steps 2-9.
December 2019	<ul style="list-style-type: none">• Added a note to ignore the database scripts released on OSDC and included a new patch number to be used.
February 2020	<ul style="list-style-type: none">• Revised the Prerequisite for Database Server
December 2020	<ul style="list-style-type: none">• Added the content for Installing a New Application for Sender & Receiver Services.

Date	Description of Change
February 2021	<ul style="list-style-type: none">• Added Database Configuration, Installing the Patches, Uninstalling Sender/Receiver Services Section.• Reorganized the content flow.
November 2021	<ul style="list-style-type: none">• Revised the Prerequisite for Database Server, Web Server and Application Clients.• Updated the Version for Sender/Receiver and FMS Upgrade Plan.
March 2022	<ul style="list-style-type: none">• Updated content to HTML format
August 2022	<ul style="list-style-type: none">• Updated the Prerequisite for Database Server, Web Server and Application Clients to include latest Windows version

1

Prerequisites

This topic explains the prerequisites for Fleet Management System (FMS) installation and upgrade.

Below are the minimum system requirements for each server type. We strongly recommend that you refer to the Cruise Compatibility Matrix at Oracle Help Center for the latest supported Operating System and Database version.

Database Server

Operating System: Microsoft Windows 2012 R2 / Microsoft Windows 2016 Standard / Microsoft Windows 2019 Standard / Microsoft Windows 2022 Standard

RAM: 32GB

Hard Disk Size: 1TB

Oracle Database version: Oracle 12c (12.2.0.1 64 bit) with Unicode (AL32UTF8) / Oracle 19c



Note:

Database Configuration:

- The Database character set can be set to Western or Unicode. However, you must ensure that SPMS and FMS Database character set are configured the same to avoid data discrepancy. For example, if the character set is set as UTF8 in SPMS Database, then it has to be the same in FMS Database.
- Similarly, the Database table column type must be configured the same in both the SPMS and FMS. For example, if the type NVARCHAR is used, then both the SPMS Database and FMS Database must be the same.
- Additionally, the data type and length of Database table columns in which data is to be transferred from/to must be the same between FMS and SPMS.

Internet Information Services (IIS) Web Server

Operating System: Microsoft Windows 2012 R2 / Microsoft Windows 2016 Standard / Microsoft Windows 2019 Standard / Microsoft Windows 2022 Standard

RAM: 16GB, Hard Disk Size: 512GB

Oracle Full Client: 12.2.0.1 32 bit / 19c

Microsoft .Net Framework: Version 4.6.1. See [Microsoft .Net Framework Version](#) for more information.

FMS Application Client

Operating System: Microsoft Windows 10 Enterprise Build 1607 (x64, Bare OS) / Microsoft Windows 11 (64 bits) / Microsoft Windows 2019 Standard / Microsoft Windows 2022 Standard

RAM: 16GB, Hard Disk Size: 512GB

Oracle Full Client: 12.2.0.1 32 bit / 19c

Microsoft .Net Framework: Version 4.6.1, see [Microsoft .Net Framework Version](#).

Java Runtime Environment (JRE): Version 8

 **Note:**

You must have JRE installed on client running the FMS Database Updater application

Network

- All the FMS Sender / Receiver host machines must be in same domain when transferring the data over MSMQ with the Active Directory integration.
- The IIS Server machine and the FMS Client machine also must be on the same domain to authenticate the login credentials in Active Directory login mode.

2

Pre-Installation Task

Before you upgrade or install the FM Suite, perform the following tasks:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Acquire Secure Sockets Layer (SSL) compliant security certificate from Certification Authority.

Read and understand the Security Overview in Oracle Hospitality Cruise Fleet Management Security Guide.

Microsoft .Net Framework Version

To verify if you have the required .Net version, perform the following steps:

1. You have to execute the below statement in the command prompt (CMD).reg query
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework
Setup\NDP\v4\full" /v version
2. If it displays the version less than 4.6.1, you need to download the .Net Framework 4.6.1 version.

3

Uninstalling Fleet Management Component or Add Ons

This section describes the un-installation steps for **Fleet Management Component** or **Add-On**.

1. Go to the following location: C:\Control Panel\All Control Panel Items\Programs and Features
2. Right-click the Fleet Management Component or Add-On you want to remove, and then select **Uninstall**
3. To make sure the component or the Add-On is uninstalled successfully, go to C:\Control Panel\All Control Panel Items\Programs and Features.

4

IIS Web Server Configuration

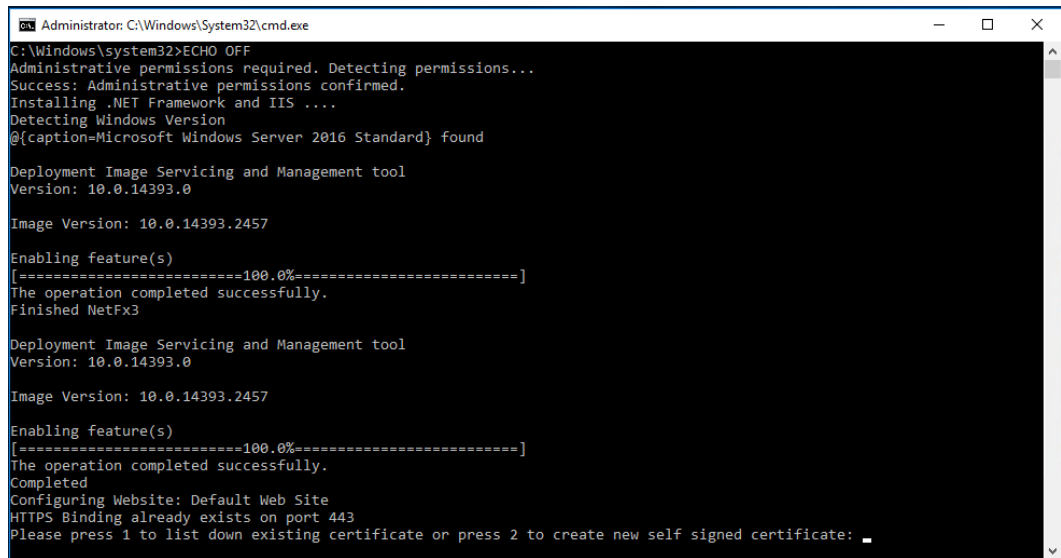
 **Note:**

For a secure communication, customers need to obtain the SSL certificates from a recognized Certificate Authority. If they fail to do so, they may use the self-signed certificates, which are vulnerable and not secure.

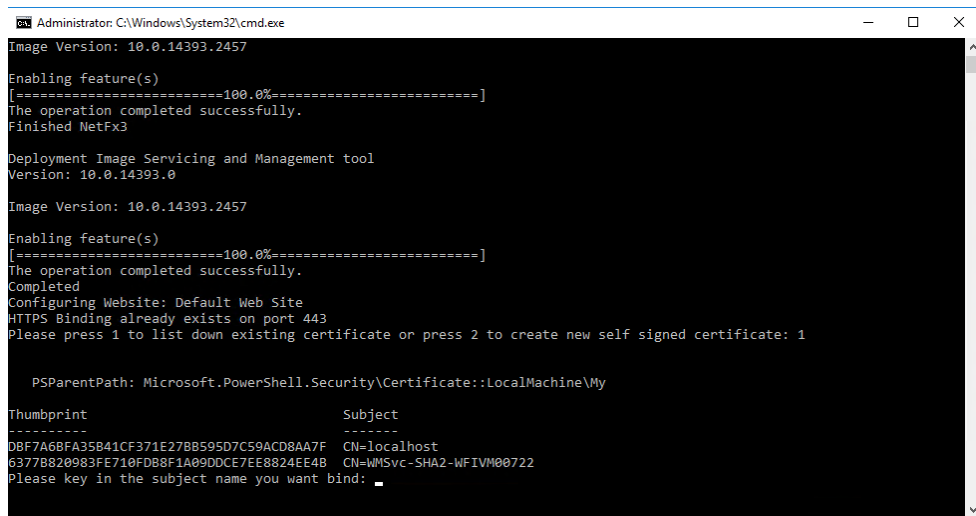
To start the IIS server, you need to create a self-signed certificate. To create a self-signed certificate and configure follow the below steps:

1. Run the Install.bat file as administrator located in the below path of the FMS version 9.1 software downloaded. \FMS Web Applications Enablement\ Install.bat.
2. Installation commences with the registration of .NET and to enable the IIS enablement. Once IIS is enabled, Hyper Text Transfer Protocol Secure (HTTPS) binding is created on port 443 and Hyper Text Transfer Protocol (HTTP) Binding is deleted on port 80.

Figure 4-1 IIS Certificate Binding



3. Process to bind certificate starts. The screen will prompt you to “Please press 1 to list down existing certificate or press 2 to create new self-signed certificate”

Figure 4-2 Certificate available for binding


```

Administrator: C:\Windows\System32\cmd.exe
Image Version: 10.0.14393.2457

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Finished NetFx3

Deployment Image Servicing and Management tool
Version: 10.0.14393.0

Image Version: 10.0.14393.2457

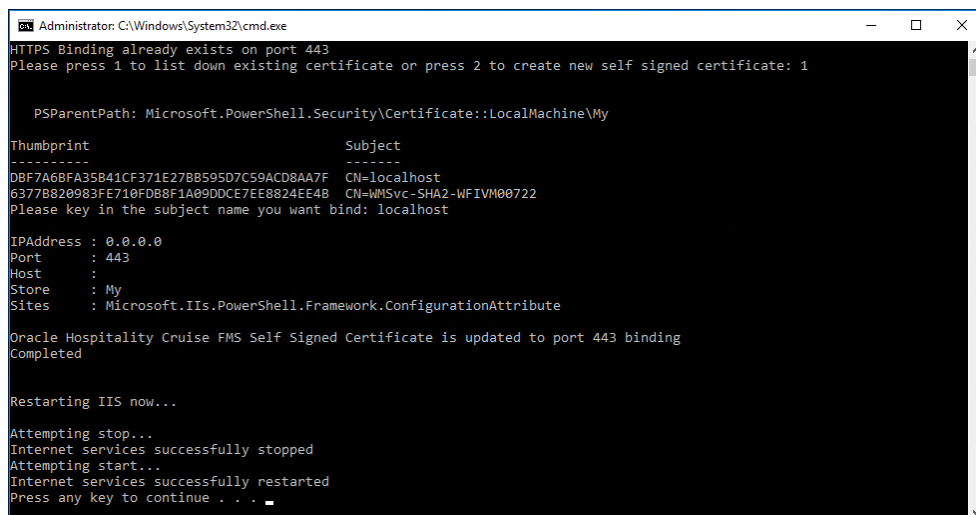
Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Completed
Configuring Website: Default Web Site
HTTPS Binding already exists on port 443
Please press 1 to list down existing certificate or press 2 to create new self signed certificate: 1

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
DBF7A6BFA35B41CF371E27BB595D7C59ACD8AA7F  CN=localhost
6377B820983FE710FDB8F1A09DDCE7EE8824EE4B  CN=WMSvc-SHA2-WFIVM00722
Please key in the subject name you want bind:

```

4. Enter 1 to list of all the existing certificates.
5. Write down the subject name to bind the certificate.
6. IIS restarts when the selected certificate is bound to port 443.

Figure 4-3 Binding IIS to Port


```

Administrator: C:\Windows\System32\cmd.exe
HTTPS Binding already exists on port 443
Please press 1 to list down existing certificate or press 2 to create new self signed certificate: 1

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
DBF7A6BFA35B41CF371E27BB595D7C59ACD8AA7F  CN=localhost
6377B820983FE710FDB8F1A09DDCE7EE8824EE4B  CN=WMSvc-SHA2-WFIVM00722
Please key in the subject name you want bind: localhost

IPAddress : 0.0.0.0
Port      : 443
Host      :
Store     : My
Sites     : Microsoft.IIS.PowerShell.Framework.ConfigurationAttribute

Oracle Hospitality Cruise FMS Self Signed Certificate is updated to port 443 binding
Completed

Restarting IIS now...

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
Press any key to continue . . .

```

7. Enter 2 and you are prompted to enter the domain or the Internet Protocol (IP) address.

Figure 4-4 Domain or Internet Protocol Address Entry

```

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>ECHO OFF
Administrative permissions required. Detecting permissions...
Success: Administrative permissions confirmed.
Installing .NET Framework and IIS ....
Detecting Windows Version
@(caption=Microsoft Windows Server 2016 Standard) found

Deployment Image Servicing and Management tool
Version: 10.0.14393.0

Image Version: 10.0.14393.2457

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Finished NetFx3

Deployment Image Servicing and Management tool
Version: 10.0.14393.0

Image Version: 10.0.14393.2457

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Completed
Configuring Website: Default Web Site
HTTPS Binding already exists on port 443
Please press 1 to list down existing certificate or press 2 to create new self signed certificate: 2_

```

Figure 4-5 Self-signed Certificate Created

```

Administrator: C:\Windows\System32\cmd.exe
Deployment Image Servicing and Management tool
Version: 10.0.14393.0

Image Version: 10.0.14393.2457

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Completed
Configuring Website: Default Web Site
HTTPS Binding already exists on port 443
Please press 1 to list down existing certificate or press 2 to create new self signed certificate: 2
Please key in your domain name or ip: localhost
Oracle Hospitality Cruise FMS Self Signed Certificate already exists

IP Address      Port  Host Name      Store      Sites
-----
0.0.0.0         443   -----
My              Default Web Site
Oracle Hospitality Cruise FMS Self Signed Certificate is updated to port 443 binding
Completed

Restarting IIS now...

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
Press any key to continue . . .

```

8. IIS restarts when the self-signed certificate is created and bound to port 443.

5

Installation of Fleet Management Component or Add-On

The following topic describes the installation steps of Fleet Management Component or Add-On

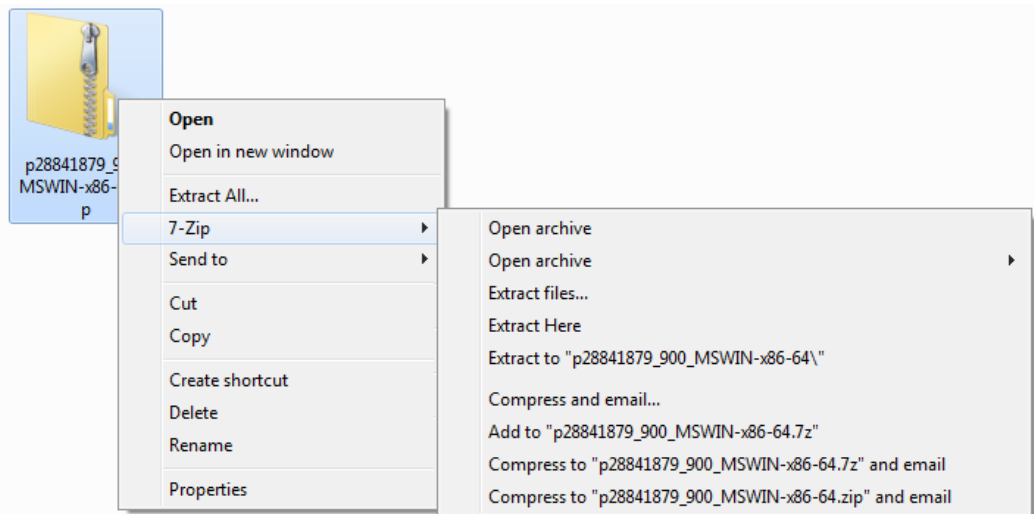


Note:

You can download the Database Schema Password Manager and the Encryption Manager tools from My Oracle Support (MOS). Both are not provided in the FMS Suite 9.1.0.0 package.

1. Download the Installation file from OSD (Oracle Software Deliver Cloud)/ MOS.
2. Extract the zip file using the **Extract Here**.

Figure 5-1 Downloaded Installation File (Zip format)



3. Open the **Setup** folder from the above extracted zip file.
4. Right-click the OHCFCM.exe and select **Run as administrator** to install the application.
5. On the Oracle Installation Welcome screen, click **Next** to continue.
6. Select **I accept the terms of the license agreement** option, and then click **Next** to install Fleet Management or click **Cancel** to cancel the installation process.

Installation Notes

1. Select the **Microsoft .NET Framework** option if the system does not have a previous installation of the .NET Framework.
 - To view a list of all installed software, open the **Control Panel**, and then select **Program and Features**. If the Microsoft.NET Framework appears in the list of installed software, do not select the **Microsoft .NET Framework** installation option.
2. Select the required Components or Add-Ons, and then click **Install**.
3. Click **Finish** to exit the installation process.

Post Installation Notes

- See **Secure Clients** section in the *FMS 9.1 User Guide* for the Security Server Configuration on FMS IIS Web Server.
- Requirement to add the IIS server machine name in config.json file (C:\inetpub\wwwroot\OHCgangwayActivityWebApp) of Gangway web application.
- To modify the value of ServiceUrl, replace localhost with the IIS machine name in ERSService.js file (C:\inetpub\wwwroot\OHCEmergencyMobileApp) of ERS web application.
- To ensure Database Schema passwords are compatible with FMS 9.1, see **Database Schema Password Manager** chapter in the *FMS 9.1 User Guide*.
- To upgrade Database to FMS version 9.1, ignore the database scripts available in installation package. **Download and run the scripts provided in patch number 30615259** instead. See *FMS 9.1 User Guide*, **Database Updater** chapter.
- When the installation is completed. Go to the specific FMS component directory, for example, C:\Program Files (x86)\Oracle Hospitality Cruise.
 - Add the ServiceURL information to each Component or Add-On .exe configuration file. See below for the example.

```
<appSettings>
  <add key="FidelioBkPwd" value=""/>
  <add key="KEKKey" value=""/>
  <add key="ServiceUrl" value="https://Host-Machine-Name/
OHCfMSSecurityService/FCTransactionsService.asmx"/>
  <add key="launcher1" value="layout_fms"/>
  <add key="launcher2" value="layout_occ"/>
  <add key="LogExceptionToFile" value="True"/>
  <add key="ClientSettingsProvider.ServiceUri" value=""/>
  <add key="IsActiveDirEnabled" value="N"/>
  <add key="isFileUpdaterEnabled" value="Y"/>
  <add key="isShipSide" value="N"/>
  <add key="Languages" value=""/>
</appSettings>
```

```
<add key="IsActiveDirEnabled" value="N"/> if Set Y for active
directory login authentication
```

```
<add key="isFileUpdaterEnabled" value="Y"/> if Set N for
```

running desktop applications e.g. Data Viewer, Corporate access Management on Windows 10.

```
<add key="isShipSide" value="N"/> if Set Y to run ship side  
interfaces (Sender, Receiver, Watchdog)
```

- Launch your application by using the application icon(s) available on desktop.

6

Performing FMS Upgrade

What You Should Know

Make sure you have an operational understanding as follows:

- Personal Computers (PCs) and a working knowledge of Microsoft Windows interface
- Understanding of basic network concepts
- Experience with Microsoft Windows Server 2012 R2
- Experience with Oracle 11g, Oracle 12c
- Microsoft Windows administrative privileges

In addition, you must know

- You cannot repair or modify installation features due to changes in the setup process. If a problem occurs, you must uninstall any installed applications and reinstall FMS.

Before You Begin

You must have the FMS version 9.0 before upgrading the FMS software, take note of the followings:

- When performing an upgrade to version 9.1, you must perform a database verification and backup task for the databases.
- Have a dedicated Client PC ready for an upgrade.
- Follow the prompts in the FMS software installation. If you cancel the installation after it starts, using any method other than through the provided prompts; the results can be unpredictable.
- You must be logged in as an administrator before running the FMS setup on a Microsoft Windows system.
- Ensure that all other programs and applications are closed on the PC. If the system detects an active program or process during the installation routine, a notification to close them may appear.

Pre-Installation Task

You must complete the tasks mentioned in chapter [Pre-Installation Task](#) before continuing

Acquiring the patches

The installation requires you to have Administrator privileges. You must acquire the patches from the My Oracle Support (MOS) site.

Table 6-1 Patch from MOS

Software	Patch Number	Patch Name
Database Scripts	29754121	Script for Shore Sender/ Receiver required FCU/FCX Entries
Database Scripts	30615259	Script Upload for FMS 9.1.0.0

Installing the patches

From FMS 9.1.2 onwards, a patch release will not contain a full setup files for FMS applications. Patch release will only contain the setup file for the FMS application to be patched. This is to ensure conformance to the Release standards to distinguish a Patch release from a Major/Minor release.

For example, in FMS 9.1.2, there will be a patch for FMS Sender and Receiver. As a pre-requisite to apply this patch, the full FMS applications must be installed using FMS 9.1.0 setup file. When that is met, the FMS 9.1.2 Sender and Receiver setup file can be run to install the patch.

Installing a New Application for Sender and Receiver Services

Note:

The **Activity Log** tab functionality to check the transfer of data will not be available when the FMS Sender and Receiver are installed as Windows Services. This is due to the inherent design of Windows Services which are not capable of refreshing UI updates.

The Sender Receiver Interfaces is a Windows Desktop application and it behaves as a configurator. User is able to select a single type of Sender to install. Once It is installed, you will obtain an executable file in the **C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS Sender** folder.

Installing a Sender Service



1. Open the InstallShield Installer, click **Next** to install a new service.
2. Click **Finish**. This closes the InstallShield Installer window.
3. Go to C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS Sender folder.
4. Open **OHC FMS Sender.exe.Config** and change ServiceUrl with **Security Services**. Then set the **isShipSide** value to 'Y' (for ships' side configuration).

Figure 6-1 Security Services Setting for Shore Side Sender

```
<?xml version="1.0"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1" />
  </startup>
  <!--<appSettings>
    <add key="FidelioBkPwd" value="" />
    <add key="KEKKey" value="" />
    'for shore side service url
    <add key="ServiceUrl" value="https://Host-Machine-Name/OHCFMSSecurityService/FCTransactionsService.asmx"/>
    |'for ship side service url
    <add key="ServiceUrl" value="https://Host-Machine-Name/OHCFMSSecurityService/OHCSecurity.asmx"/>
    <add key="LogExceptionToFile" value="True"/>
    <add key="IsActiveDirEnabled" value="N"/>
    <add key="isShipSide" value="N"/>
  </appSettings-->
  <appSettings>-->
    <add key="FidelioBkPwd" value="" />
    <add key="KEKKey" value="" />
    <add key="ServiceUrl" value="https://Host-Machine-Name/OHCFMSSecurityService/FCTransactionsService.asmx" />
    <add key="LogExceptionToFile" value="True" />
    <add key="IsActiveDirEnabled" value="N" />
    <add key="isShipSide" value="N" />
  </appSettings>
</configuration>
```

Figure 6-2 Security Services Setting for Ship Side Sender

```

<?xml version="1.0"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1"/>
  </startup>
  <!--appSettings-->
  <add key="FidelioBkPwd" value="" />
  <add key="KEKKey" value="" />
  <!--for shore side service url-->
  <add key="ServiceUrl" value="https://Host-Machine-Name/OHCFMSSecurityService/FCTransactionsService.asmx"/>
  <!--for ship side service url-->
  <add key="ServiceUrl" value="https://Host-Machine-Name/OHCTransactionsService/OHCSecurity.asmx"/>
  <add key="LogExceptionToFile" value="True"/>
  <add key="IsActiveDirEnabled" value="N"/>
  <add key="isShipSide" value="N"/>
</appSettings-->
<appSettings>
  <add key="FidelioBkPwd" value="" />
  <add key="KEKKey" value="" />
  <add key="ServiceUrl" value="https://Host-Machine-Name/OHCTransactionsService/OHCSecurity.asmx" />
  <add key="LogExceptionToFile" value="True" />
  <add key="IsActiveDirEnabled" value="N" />
  <add key="isShipSide" value="Y" />
</appSettings>
</configuration>

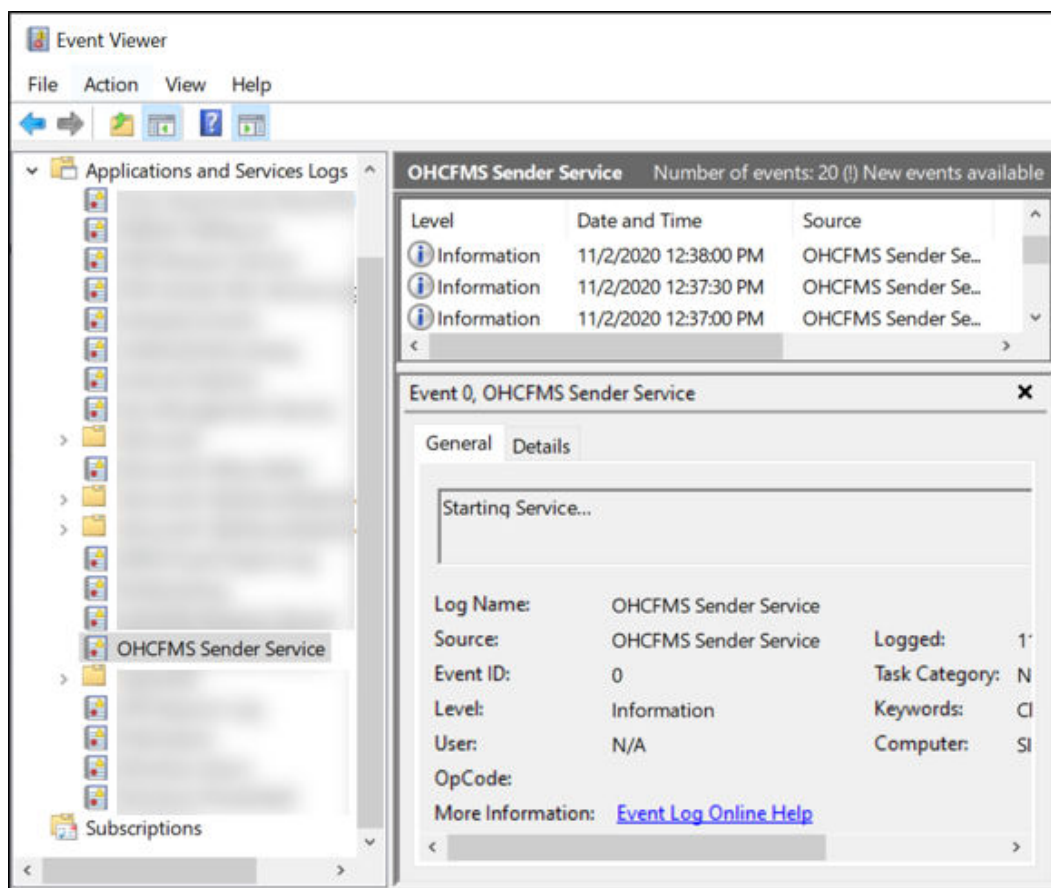
```

5. Open the sender configuration from the desktop's shortcut (OHC FMS Sender.exe).
6. Enter the application login credential. Key in the required information for **Login** and **Password**. From the drop-down list, select **TNS Names file** and **Data Source**.
7. Click **OK** to log in.
8. Select the default schema and click **Apply**.
9. Create a new schedule task for the Sender. Any changes of the scheduled tasks requires a restart of the service.

Figure 6-3 New Schedule Task for Sender

10. Open the Services application
 - Click **Start**.
 - Type **Services**.
 - **Click** or **tap** the matching result.
11. Select OHC FMS Sender, and click **Start Service**.
12. In the Event Viewer, you are able to check the status of the service

Figure 6-4 Event Viewer — Sender Services



Installing a Receiver Service

1. Open the InstallShield Installer, click **Next** to install a new service.
2. Click **Finish**, this will close the InstallShield Installer window.
3. Go to C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS Receiver folder.
4. Open OHC FMS Receiver.exe.Config and change ServiceUrl with **Security Services**. Then set the isShipSide value to **'Y'** (for ships' side configuration).
5. Open the receiver configuration from the desktop's shortcut (OHC FMS Receiver.exe).
6. Enter the application login credential. Key in the required information for **Login** and **Password**. From the drop-down list, select **TNS Names file** and **Data Source**.

7. Click **OK** to log in.

Installing Sender/Receiver Application

If you do not want to install FMS Sender or FMS Receiver as a Windows Service, you can install it as a Windows Application.

1. Locate and run **OHCFMSSenderUpdate.exe** or **OHCFMSReceiverUpdate.exe**
2. Click **Update** to install.
3. Upon completion, click **Finish** to close the Patch Installer window.

Uninstalling Sender/Receiver Services

1. Go to Windows Control Panel, Add & Remove Program.
2. Search for **“OHC FMS Sender/Receiver Service”**.
3. Click on the **Uninstall** button to remove the Sender/Receiver Services.

Updating Sender/Receiver

When you are ready to update the sender/receiver, make sure you perform the followings:

1. Take a backup for “Settings.xml” and “Configsettings.xml”.
2. Uninstall the Sender/Receiver.
3. Update Sender/Receiver as follows
 - a. Upgrade shore-side FMS Sender/Receiver to 8.2.2.1006 if current version is older. (Older versions can't be upgraded directly to 8.2.2.1008).
 - b. Upgrade shipboard FMS Sender/Receiver to 8.2.2.1006 if current version is older. (Older versions can't be upgraded directly to 8.2.2.1008).
 - c. Upgrade ODAC v11.2.2 to ODAC 11.2.3.20 32 bit on FMS Sender/Receiver machine(s) shore side
 - d. Run the Database scripts for version 8.2.2.1008 provided in patch number **29754121** - Script for Shore Sender/Receiver required FCU/FCX Entries.

Important:

Prior to the running the DB Scripts, ensure all DB schemas are identified by a standard password.

- e. Post execution, ensure entries in FIDELIOBK.FCX table is as follow:

Table 6-2 FIDELIOBK.FCX

FCU_USER	FCU_DBP	FCU_ENCRY PT	FCU_EXPIRY DATE	FCU_TYPE	FCU_GRACE _ PERIOD
Schema Name	4D52EBC35D C44F8EEA91 B319925E263 0	F903D9FC63 D06D9D07D0 C8384DDE9E 1C6124372E9 41F901617 53C555FD0E FA80	31-Dec-99	1	14

- f. Also, ensure the **FIDELIOBK.FCX** table is as follow:

FCX_SECONDKEY

567330B8F5CADC10CB13A2ACA4C9487714BBADEA0B551224FB14660B41C09B87

- g. Upgrade shore-side Receiver/Sender to 8.2.2.1008.
- h. Upgrade ODAC v11.2.2 to ODAC 11.2.3.20 32 bit on FMS Sender/Receiver machine(s) shipside
- i. For Receiver/Sender to 8.2.2.1008, you need to upgrade each ship individually.

Upgrading to FMS 9.1

To upgrade your current FMS version to FMS version 9.1, you need to do as follows:

1. Upgrade FMS 8.x Server DB from 11g to 12.2c
2. Download the required patches from MOS locations using the URLs mentioned in [Acquiring the patches](#).
3. Upgrade the database with the scripts provided in patch number **30615259**. See the **Database Updater** chapter in the *FMS 9.1 User Guide*.

 **Note:**

Ignore the Database scripts available in package downloaded from OSDCloud (Oracle Software Delivery Cloud).

4. Setup the shore side FMS IIS Security Server.
5. It is recommended that you source one SSL certificate for the Security Server.
6. Follow the steps mentioned in [Updating Sender/Receiver](#). See [FMS Upgrade Plan](#) for details to upgrade.
7. When you have completed Step 5 in FMS Upgrade Plan, you need to change the schema password of all the schemas using Database Schema Password Manager. See **Database Schema Password Manager** chapter in the *FMS 9.1 User Guide*.

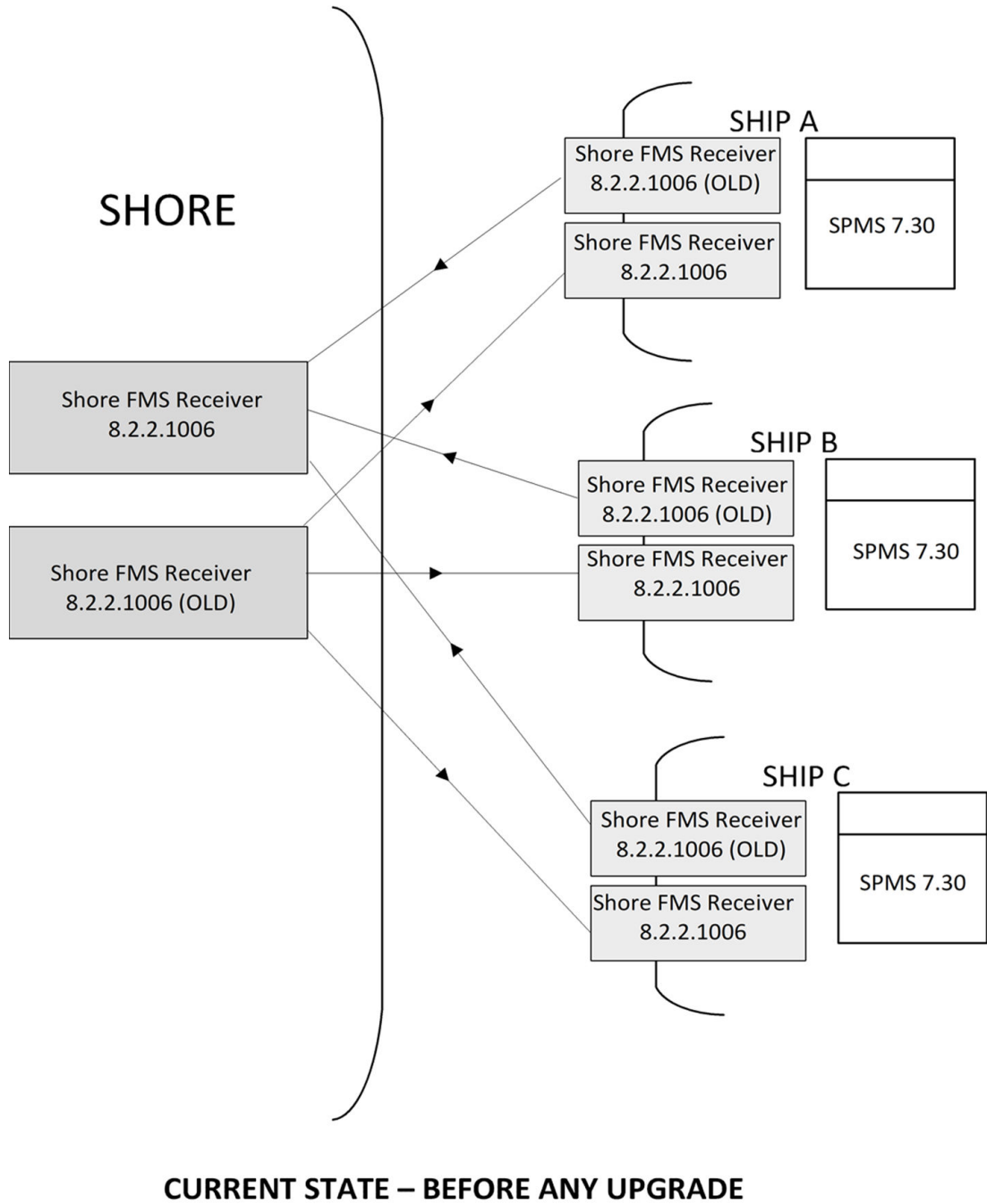
 **Note:**

To make sure the password is new and rotates regularly, you must set the System User (SYSTEM) login credentials to use the Database Schema Password Manager.

8. Continue with Step 6 in FMS Upgrade Plan.
9. Upgrade FMS applications from 8.x to 9.x
 - Data Viewer/Corporate Access Module (CAM)
 - Emerg, ResOnline (ROL)
 - Corporate Data Transfer Interface (CDTI)
 - Web-Services
 - Universal Check In (FCUCI))
10. For upgradation process refer below sections
 - [Uninstalling Fleet Management Component or Add-On](#)
 - [Installation of Fleet Management Component or Add-On](#)
11. Run the Encryption Manager (EM) and you can run it in the background. See topic [Encryption Manager in FMS 9.1 User Guide](#)

FMS Upgrade Plan

Figure 6-5 Diagram of FMS before an upgrade

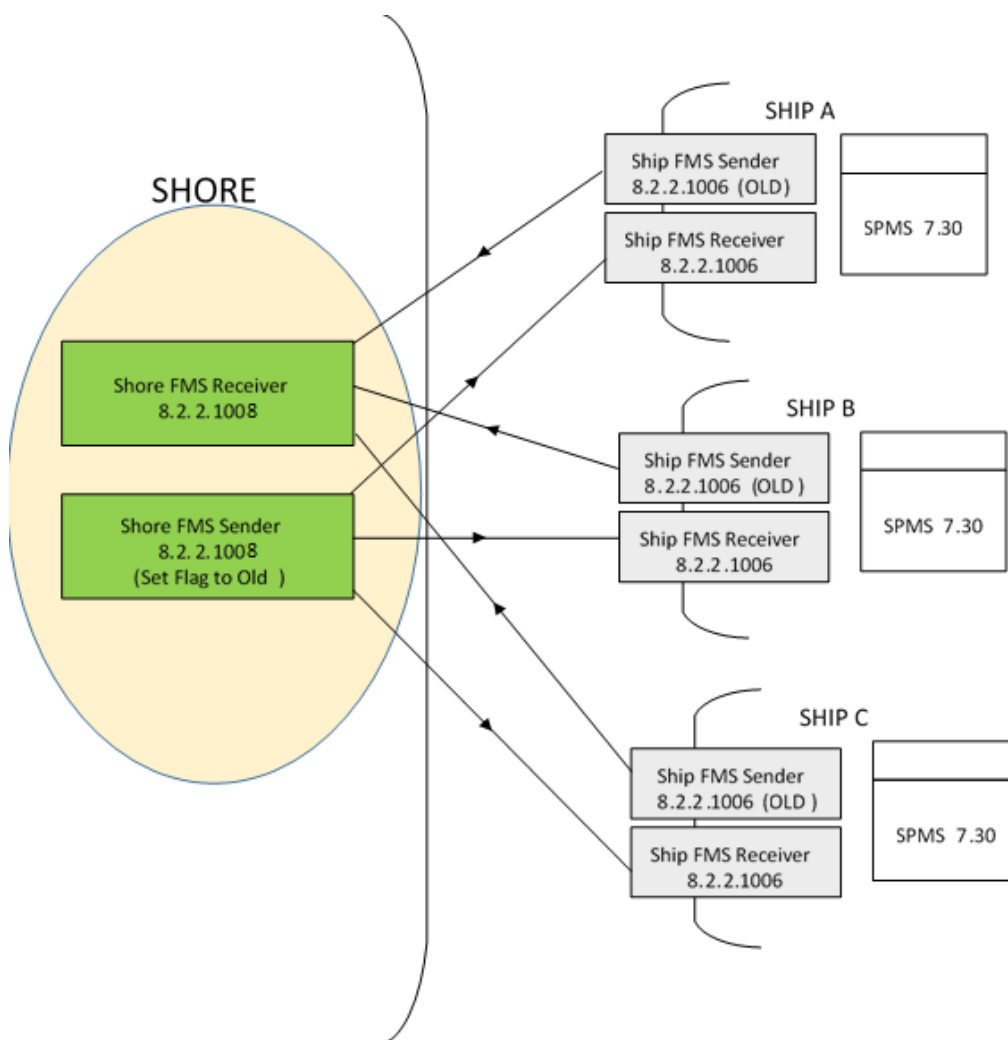


The following upgrade plan assumes there are three (3) ships in the fleet

- You must complete step 1 before continue to Step 2, 3, or 4.
- You can perform Step 2, 3 and 4 in any order and for various ships. It does not need to be at the same time.
- Continue with step 4 until step 6 in order until complete.
- You can perform Step7, 8 and 9 in any order and for various ships. It does not need to be at the same time.
- The sender configuration file is named as FMSSender.exe.Config in the application folder.

Step 1

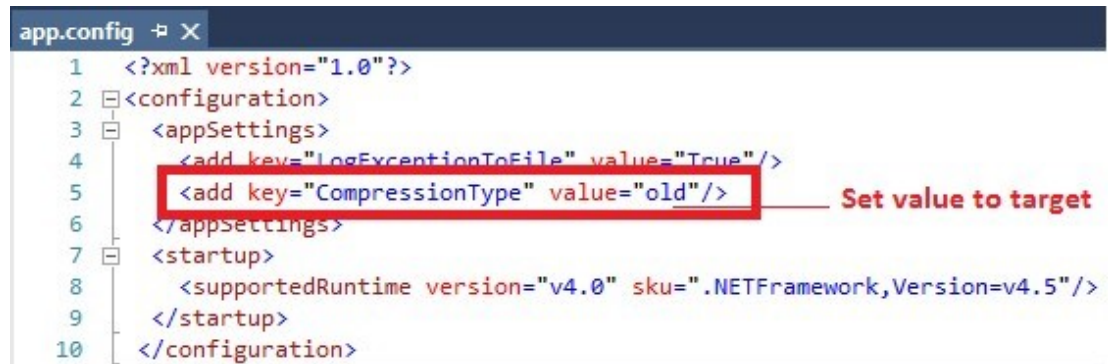
Figure 6-6 FMS Upgrade Step 1



- Install version 8.2.2.1008 Sender & Receiver shore-side to replace the old Sender & Receivers.

- In the shore-side Sender s APP.CONFIG file, set the **Compression Flag** to Old (Case Insensitive).

Figure 6-7 Upgrade Plan Step 1 Configuration

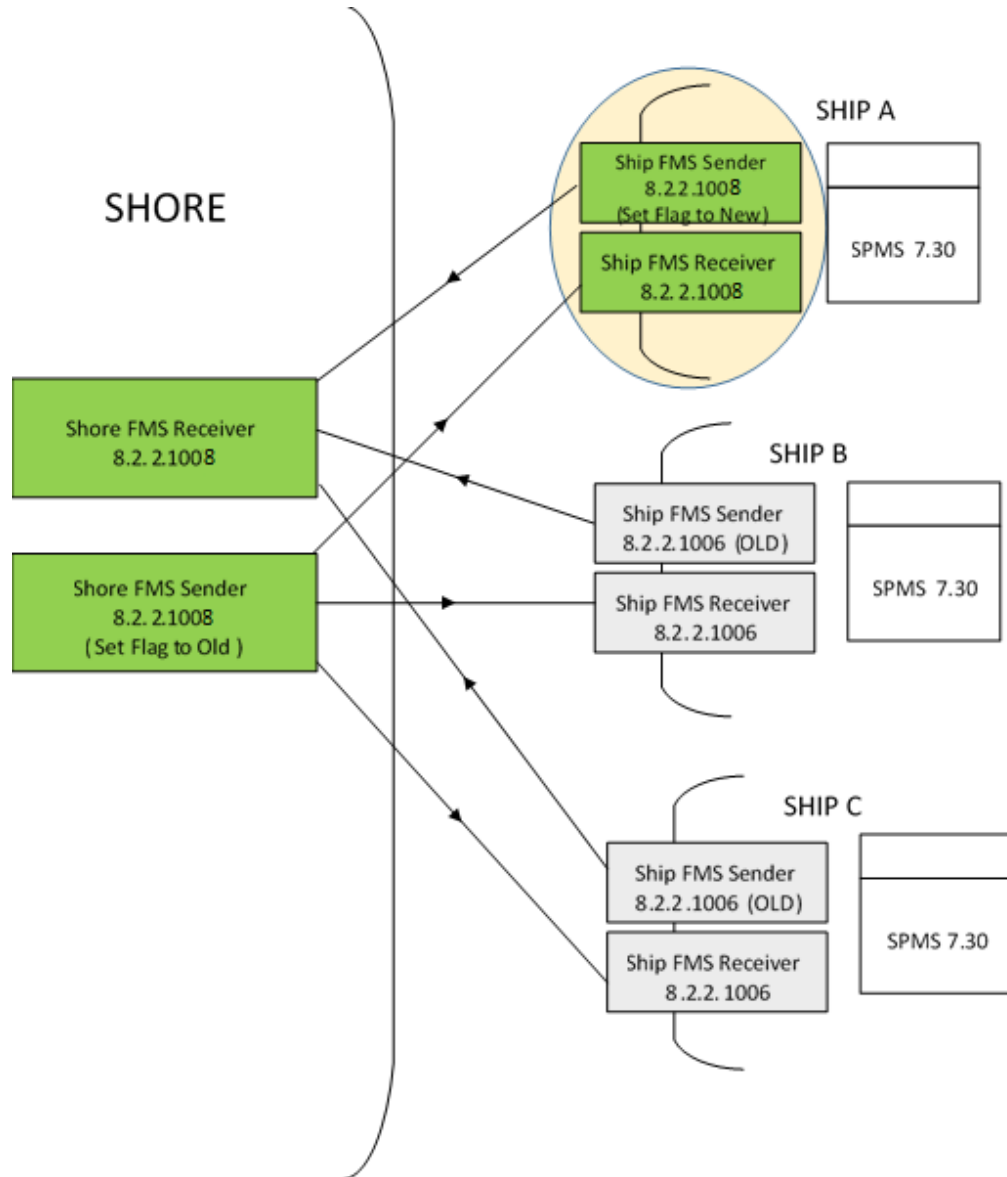


```
app.config  X
1  <?xml version="1.0"?>
2  <configuration>
3  <appSettings>
4  <add key="LogExceptionToFile" value="True"/>
5  <add key="CompressionType" value="old"/>
6  </appSettings>
7  <startup>
8  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5"/>
9  </startup>
10 </configuration>
```

Set value to target

Step 2

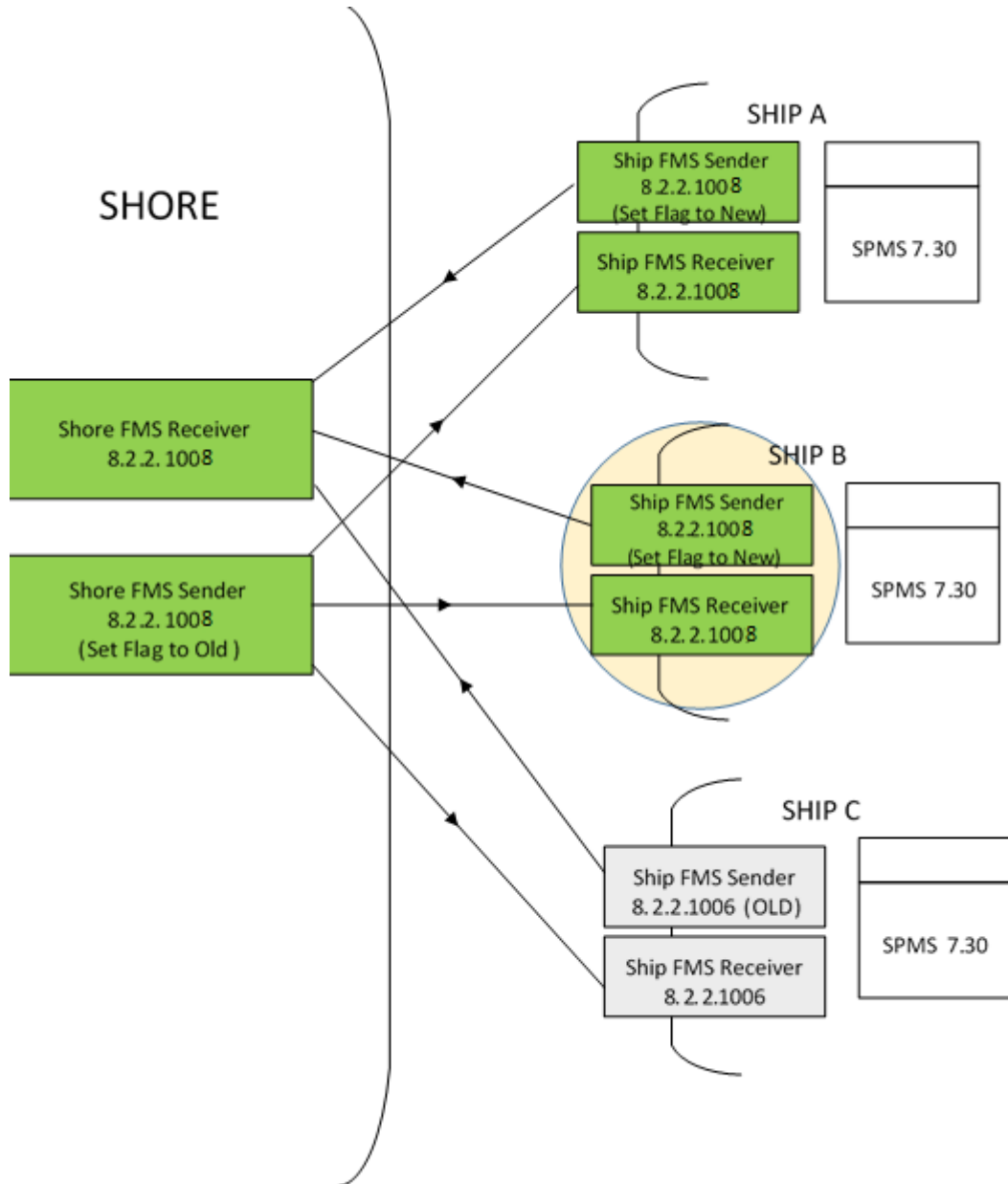
Figure 6-8 Upgrade Plan Step 2



- Install version 8.2.2.1008 Sender & Receiver on Ship A to replace the old Sender & Receivers.
- In Ship A Sender FMSSender.exe.Config file, set the **Compression Flag** to New (Case Insensitive).

Step 3

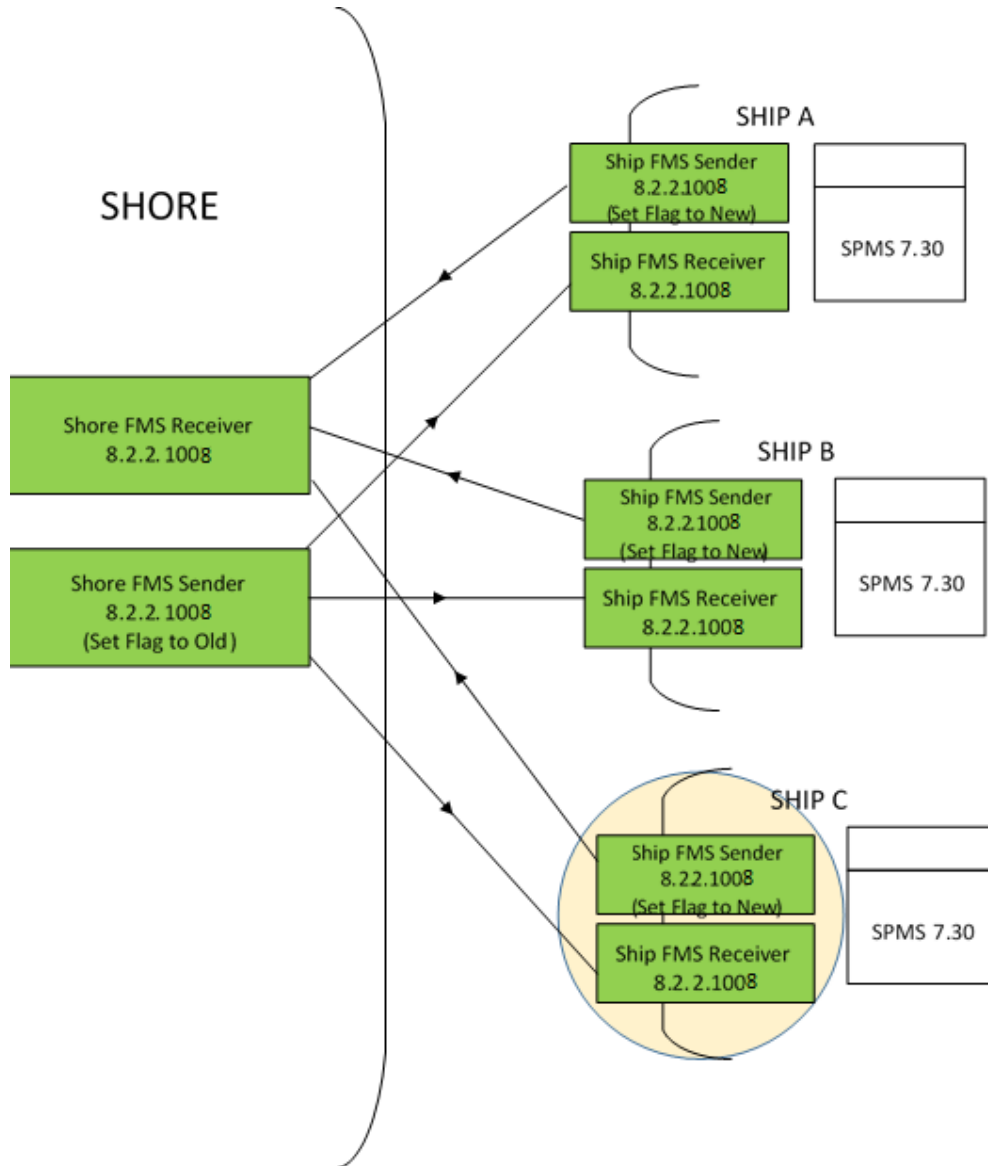
Figure 6-9 FMS Upgrade Step 3



- Install version 8.2.2.1008 Sender & Receiver on Ship B to replace the old Sender & Receivers.
- In Ship B Sender FMSSender.exe.Config file, set the **Compression Flag** to New (Case Insensitive).

Step 4

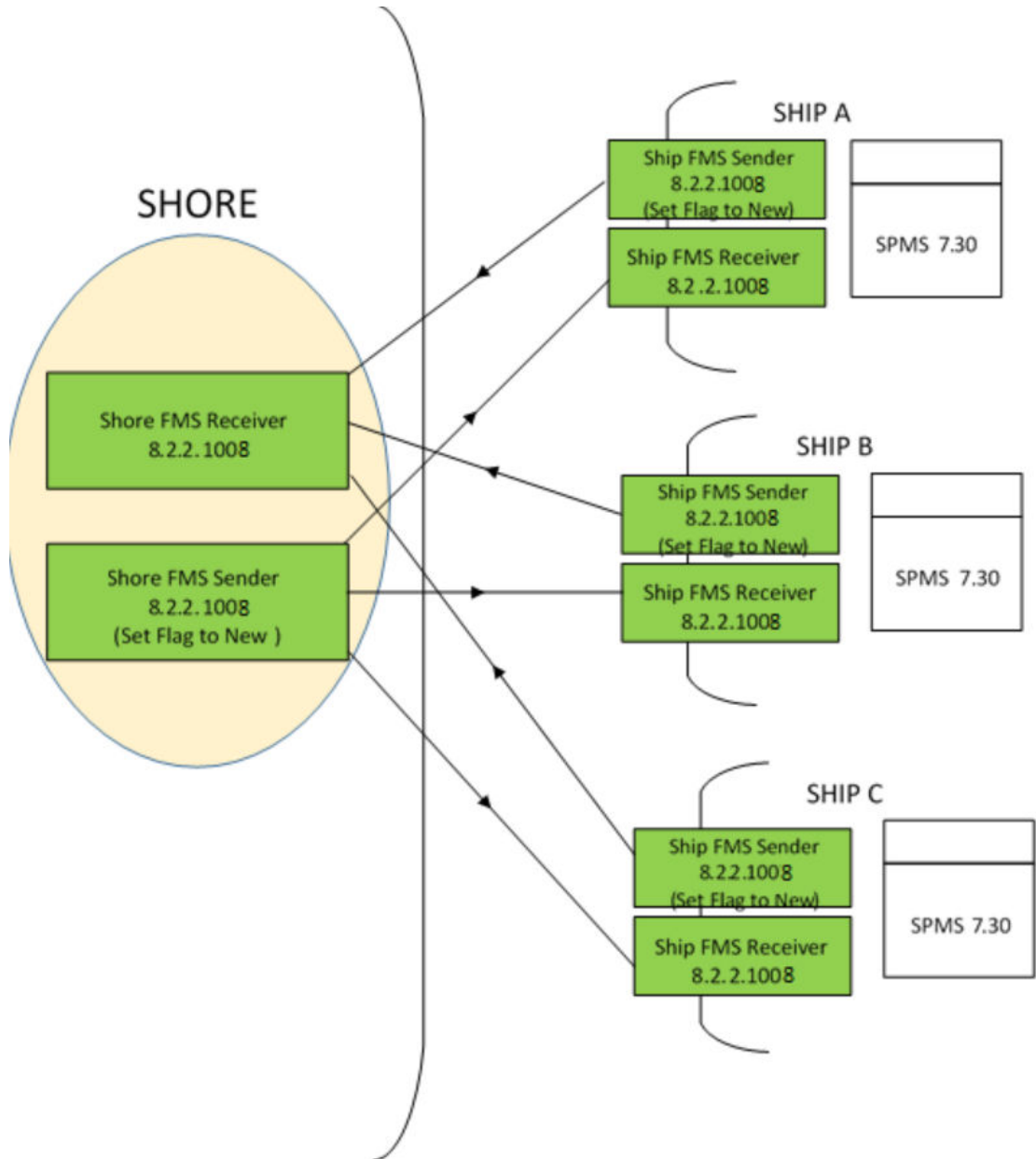
Figure 6-10 FMS Upgrade Step 4



- Install version 8.2.2.1008 Sender & Receiver on Ship C to replace the old Sender & Receivers.
- In Ship B Sender FMSSender.exe.Config file, set the **Compression Flag** to New (Case Insensitive).

Step 5

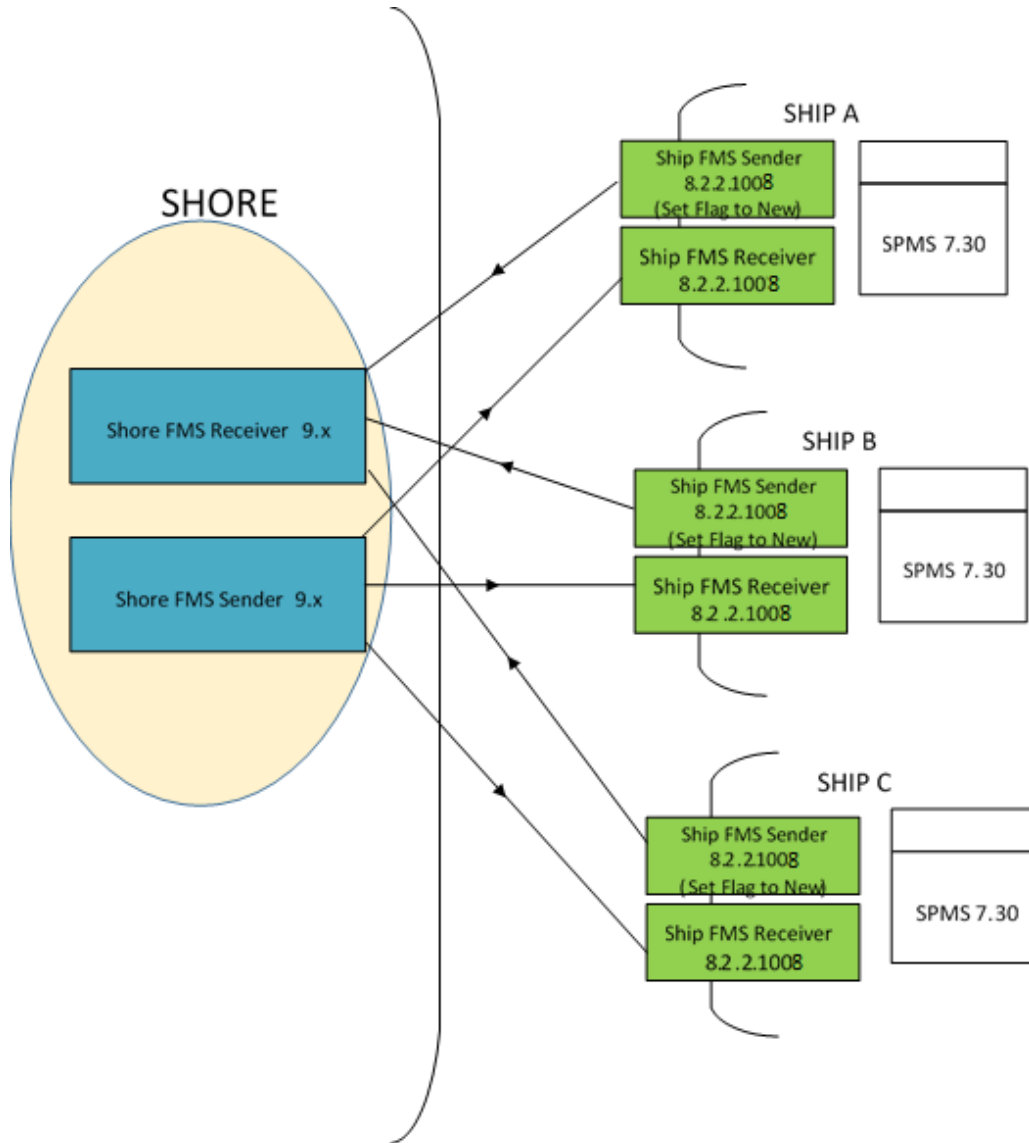
Figure 6-11 FMS Upgrade Step 5



- In the shore-side Sender FMSSender.exe.Config file, set the **Compression Flag** to New (Case Insensitive) and re-start the Sender.
- This step completes the upgrade process to 8.2.2.1008 across the fleet.

Step 6

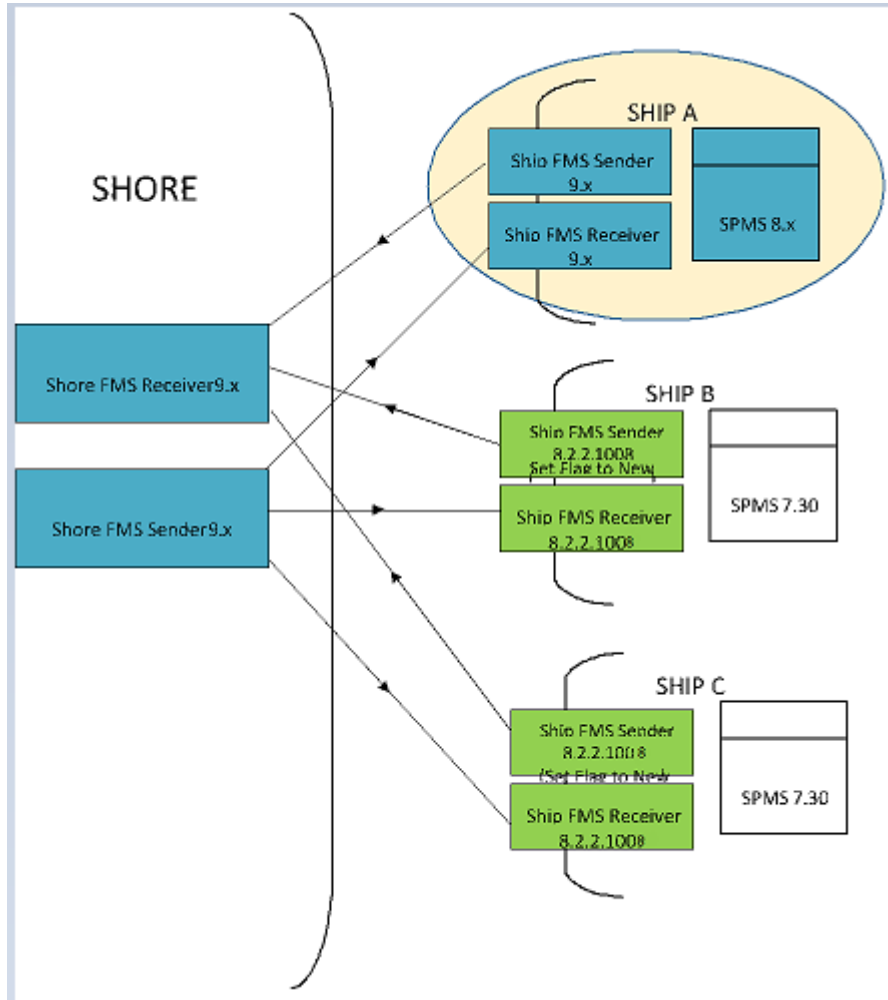
Figure 6-12 FMS Upgrade Step 6



- Before replacing shore-side Sender and Receiver to 9.x, execute the FMS Encryption Manager scripts - (FCONSOL_FMSEncryptionManager.sql) released with 9.1 version.
- Upgrade FMS to version 9.x and replace shore-side Sender and Receiver to version 9.x.

Step 7

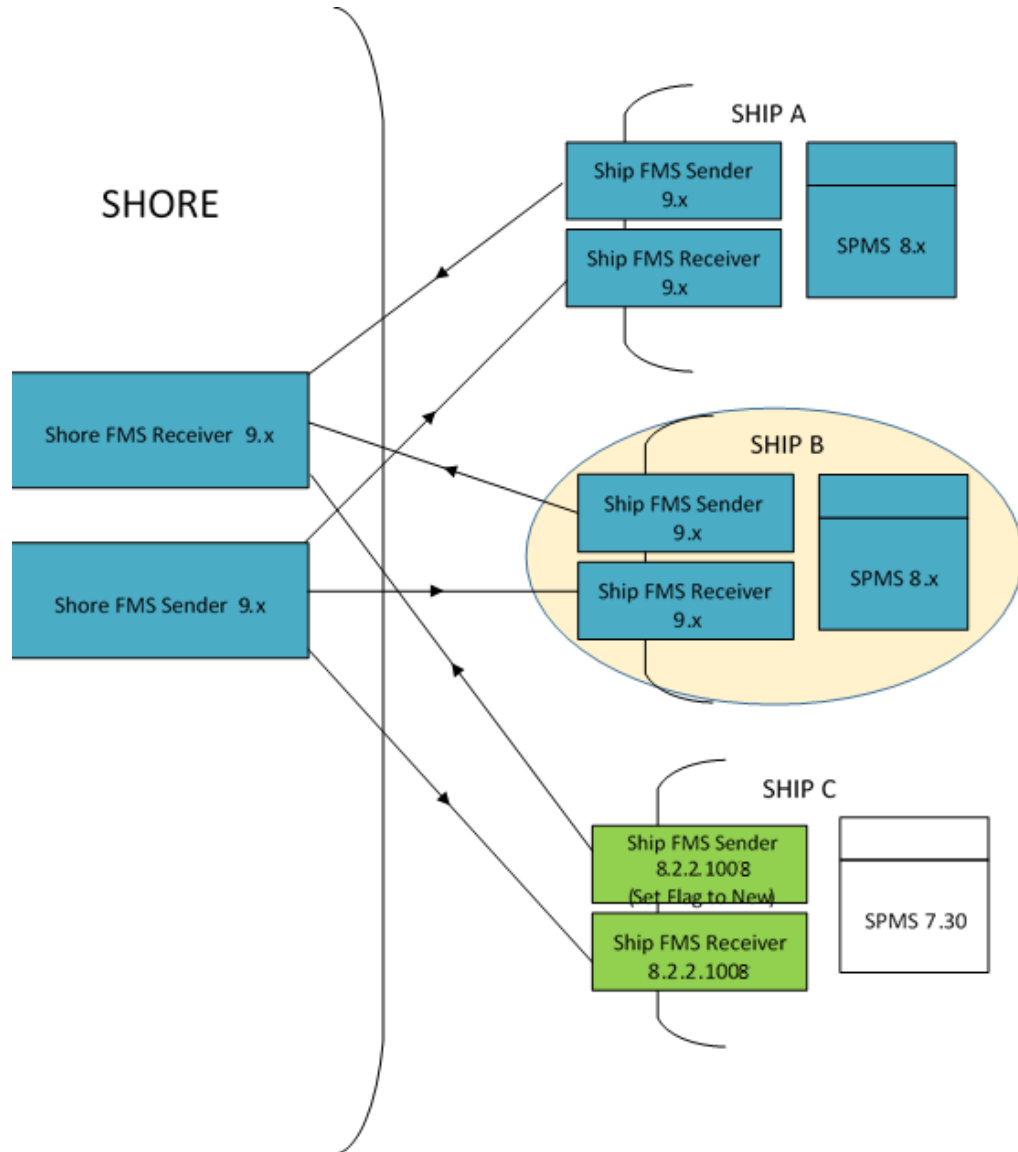
Figure 6-13 FMS Upgrade Step 7



- Upgrade SPMS to version 8.x on Ship A.
- Replace Sender and Receiver to version 9.x on Ship A.

Step 8

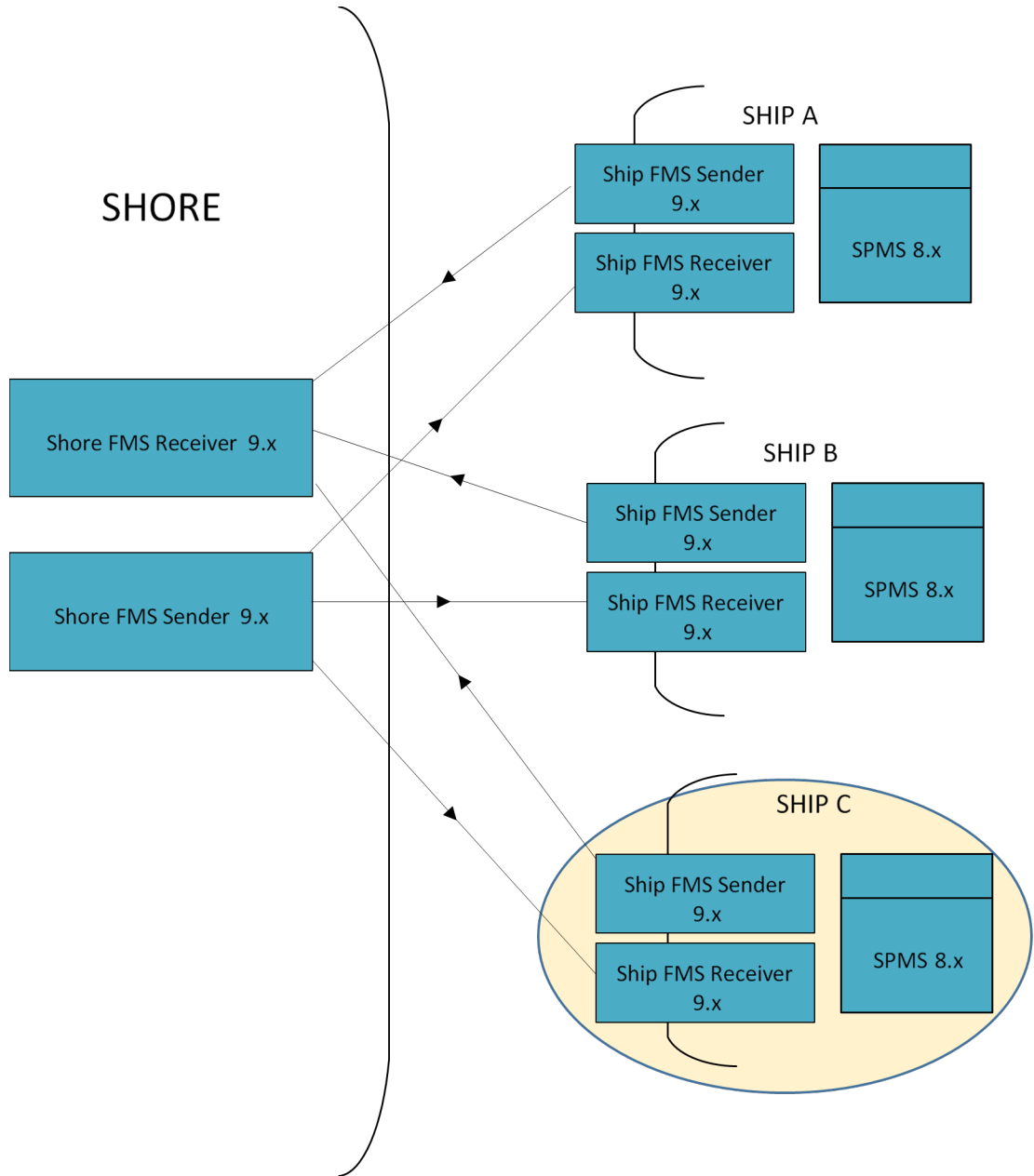
Figure 6-14 FMS Upgrade Step 8



- Upgrade SPMS to version 8.x on Ship B.
- Replace Sender and Receiver to version 9.x on Ship B.

Step 9

Figure 6-15 FMS Upgrade Step 9



- Upgrade SPMS to version 8.x on Ship C.
- Replace Sender and Receiver to version 9.x on Ship C.