Oracle® Hospitality Cruise Fleet Management System

Installation and Upgrade Guide
Release 9.0
E89562-05

April 2019

ORACLE

Contents

Figures 5

Preface 6

Audience 6

Documentation 6

Revision History 6

1 Getting Started 7

What You Should Know 7

Before You Begin 7

2 Prerequisites 8

Prerequisite for Database Server: 8

Prerequisite for IIS Web Server: 8

IIS Configuration on Windows 2012 8

IIS Configuration for Windows 2016 10

Creating a Certificate 14

Prerequisite for FMS Application Client: 18

Upgrading the Software 19

Updating the Database 19

3 Pre-Installation Task 20

4 Uninstalling Fleet Management Component or Add-On 21

5 Performing a Secure FMS Installation 22

Installation Notes 23

Post-installation Notes 24

6 Performing FMS Upgrade 25

Upgrading to FMS 9.0 25

Changing the Database Password 25

7 FMS Upgrade Plan 26

Step 1 27

Step 2 28

Step 3 29

Step 4 30

Step 5 31

Step 6 32

Step 7 33

Step 8 34
Step 9 35

Figures

Figure 2-1 - Process to bind certificate....8
Figure 2-2 - Chosen certificate is bound....9
Figure 2-3 - Restarting Internet Information Services (IIS)....9
Figure 2-4 – Enter the domain or the Internet Protocol (IP) Address....10
Figure 2-5 - Self-signed certificate is created....10
Figure 2-6 - Roles required for Security Server....11
Figure 2-7 - Features required for Security Server....13
Figure 2-8 - Default App Pool Advanced Settings for Security Server.....14
Figure 2-9 - Process to Bind Certificate....15
Figure 2-10 - Chosen Certificate Is Binded....15
Figure 2-11 - Restarting Internet Information Services (IIS)....16
Figure 2-12 - Enter Domain or Internet Protocol (IP) Address....16
Figure 2-13 - Self-signed Certificate Created....17
Figure 5-1- File Extraction....22
Figure 5-2 – OHCFM Application Installation....22
Figure 5-3 – Oracle Welcome Screen....23
Figure 5-4 – License Agreement....23
Figure 5-5 – Installation Completed....24

Preface

Oracle Hospitality Cruise Fleet Management System (FMS) provides comprehensive information on fleet performance. It integrates the database and web servers in order to provide shore-side users the access to the ship information.

The integration process involves the installation and the upgrade process of the FMS Components and Add-Ons, described herein.

Audience

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

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 and any associated log files
- Screen shots of each step you take

Documentation

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

Revision History

Date	Description of Change
March 2017	▪ Initial publication. ▪ Added two notes.
April 2018	▪ Formatting updates.
September 2018	▪ Added Upgrade information.
January 2019	▪ Updated the Prerequisite section ▪ Updated the Upgrade section
March 2019	▪ Updated the Prerequisite section ▪ Updated the Updating the Database section
April, 2019	▪ Revised the Prerequisite for Database Server ▪ Revised the Prerequisite for IIS Web Server

1 Getting Started

What You Should Know

Ensure you have an operational understanding of:

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

Knowing that:

- 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

Please keep handy the User manual of FMS for any reference Hospitality Cruise Fleet Management User Guide.

Before upgrading the FMS software, take note of the following:

- When performing an upgrade to version 9.x, 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.

2 Prerequisites

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

Prerequisite for Database Server:

Operating System: Microsoft Windows 2012 R2

RAM: 32GB, Hard Disk Size: 1TB

Oracle Database version: Oracle 11g or Oracle 12c

Prerequisite for IIS Web Server:

Operating System: Microsoft Windows 2012 R2

RAM: 16GB, Hard Disk Size: 512GB

IIS Configuration on Windows 2012

To start the IIS server, you need to create a self-signed certificate. To create a self-signed certificate:

1. Run the `Install.bat` file as the administrator located in FMS Web Applications Enablement folder (part of zip file downloaded from MOS). Installation will start with registration of `.NET` followed by 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.

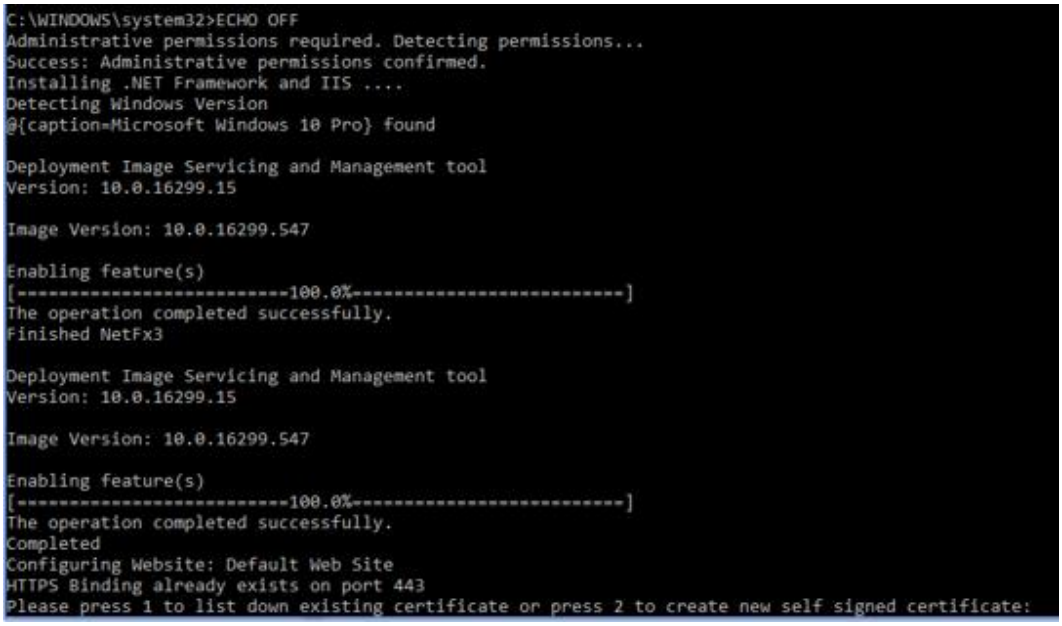


Figure 2-1 - Process to bind certificate

2. When the process to bind certificate starts; the screen will prompt you to enter `1` to view all existing certificates or enter `2` to create new self - signed certificate.

3. Enter `1` to view of all existing certificates.
4. Enter the subject name to bind the certificate.

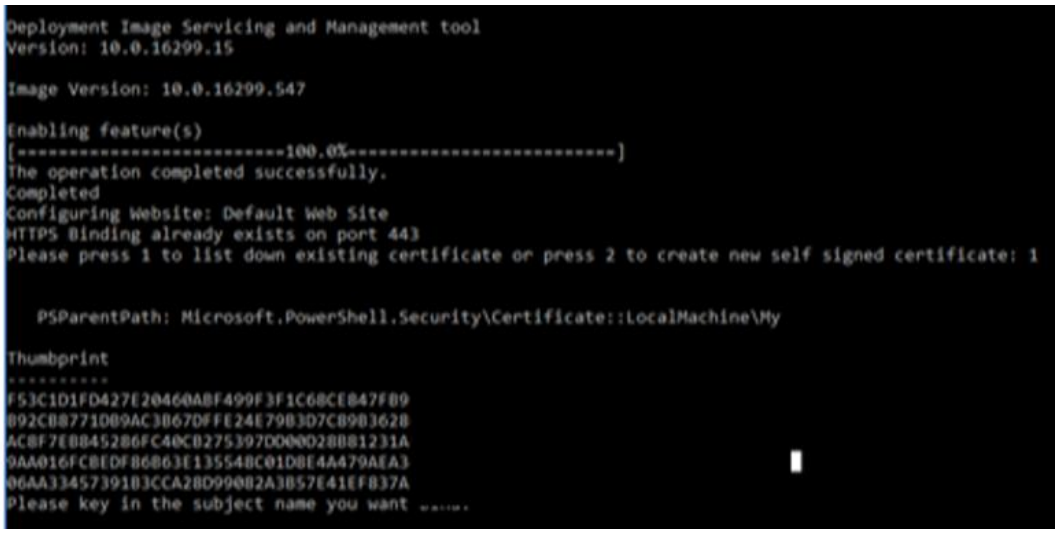


Figure 2-2 - Chosen certificate is bound

5. The chosen certificate is bind to port 443. IIS will be restarted.

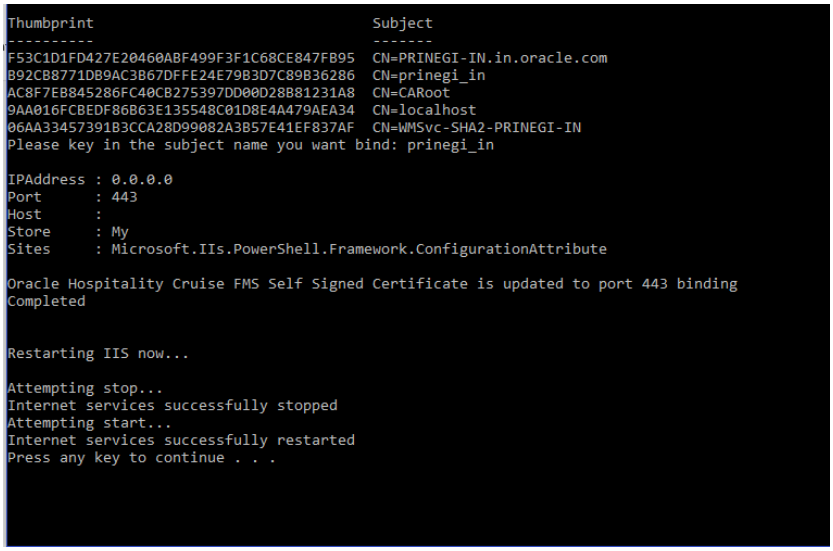


Figure 2-3 - Restarting Internet Information Services (IIS)

6. Enter 2 and it prompts you to enter the domain or the Internet Protocol (IP) address.

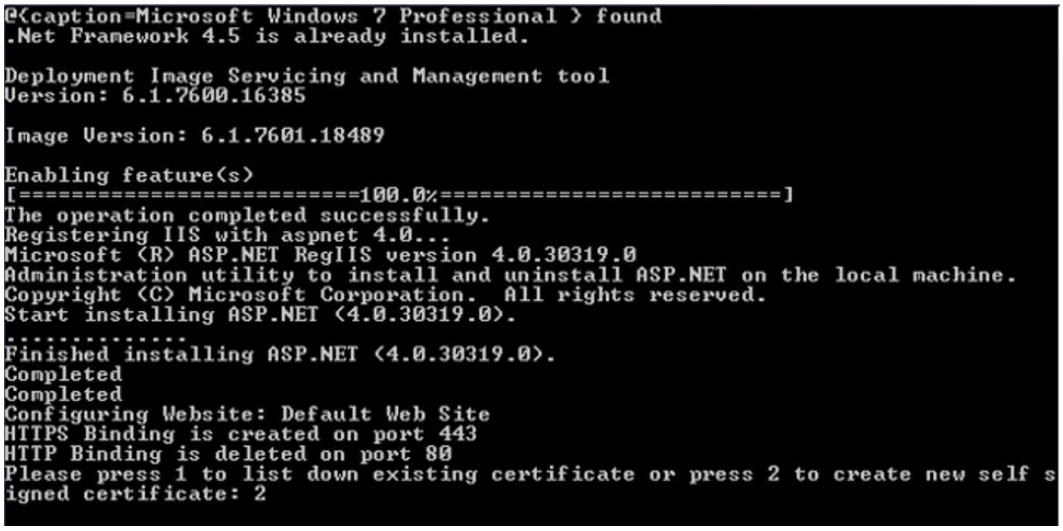


Figure 2-4 – Enter the domain or the Internet Protocol (IP) Address

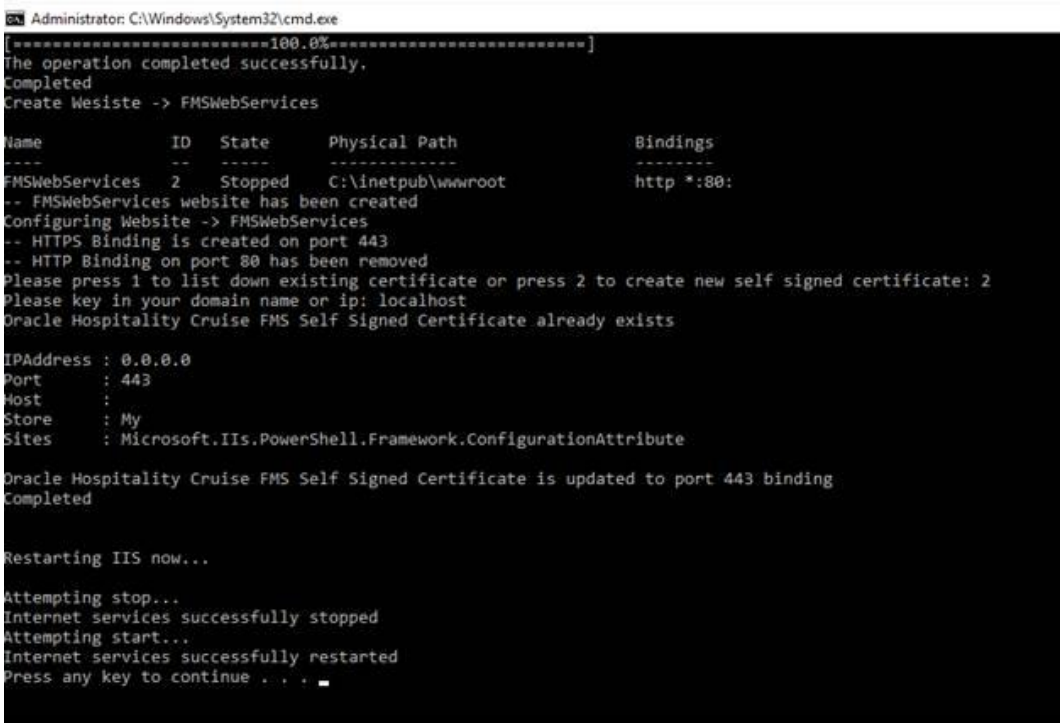


Figure 2-5 - Self-signed certificate is created

7. Self-signed certificate is created and bound to port 443. IIS will be restarted.

IIS Configuration for Windows 2016

1. **Roles:** Install the selected roles in following figure.

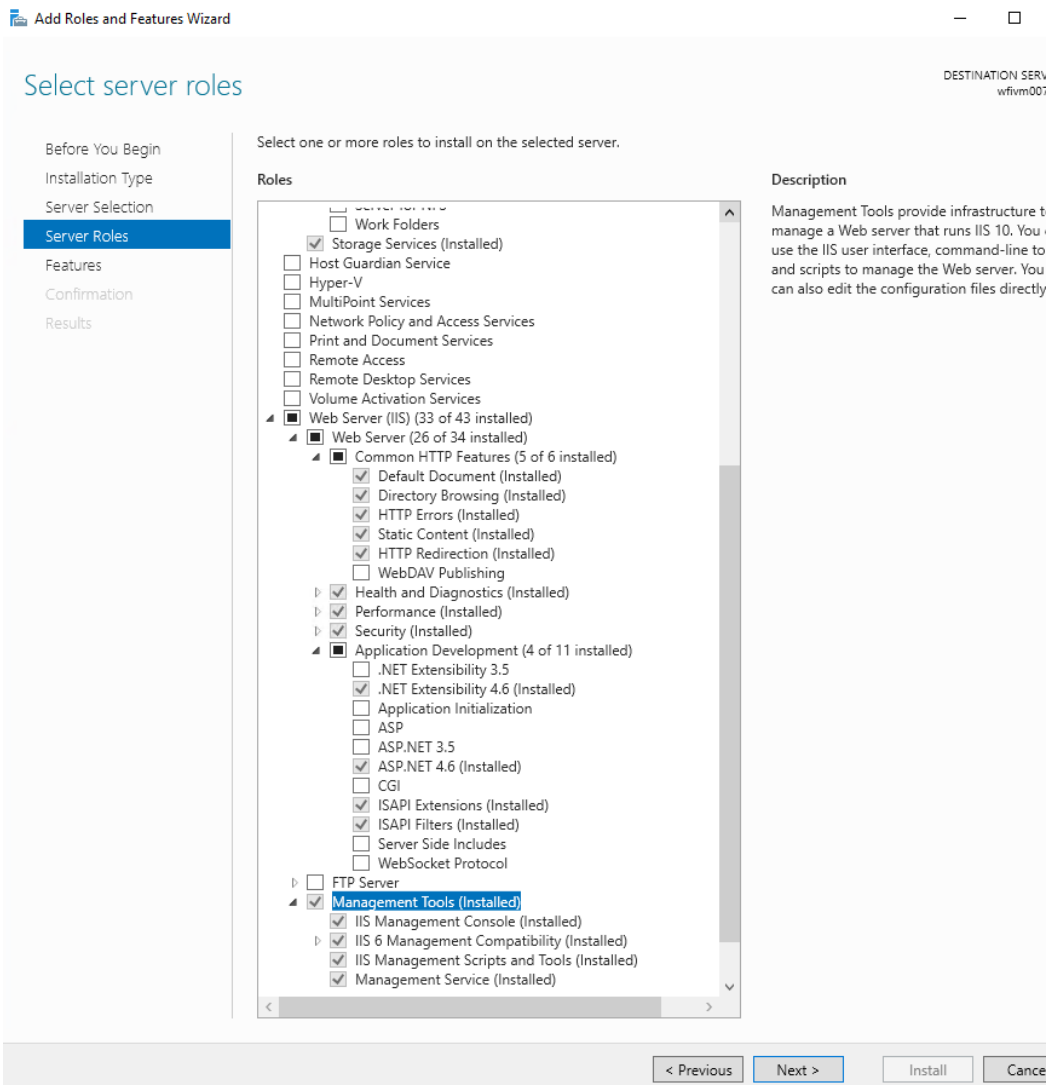
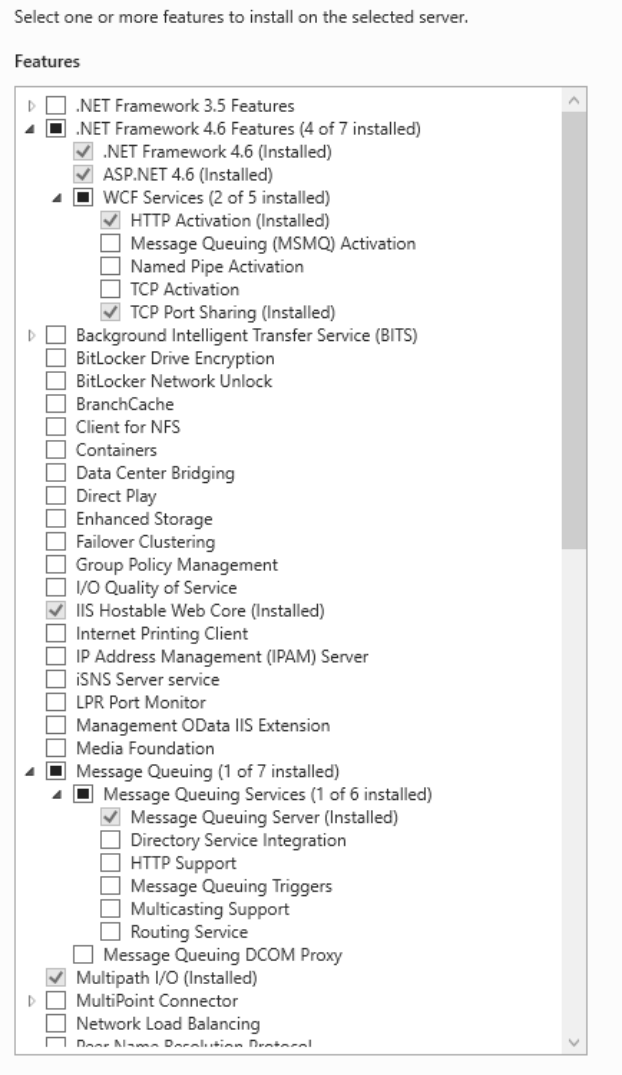


Figure 2-6 - Roles required for Security Server

2. **Features:** Install the selected features in the following figure.



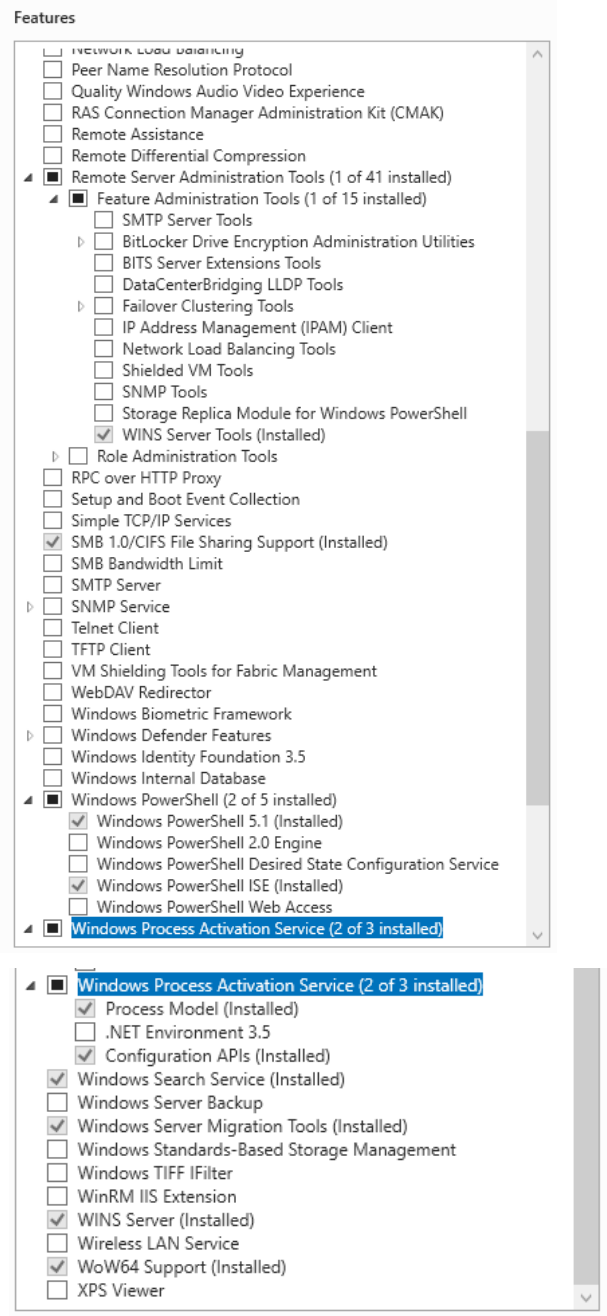


Figure 2-7 - Features required for Security Server

3. **App Pool Settings:** Default App Pool Advanced settings in IIS server in the following figure.

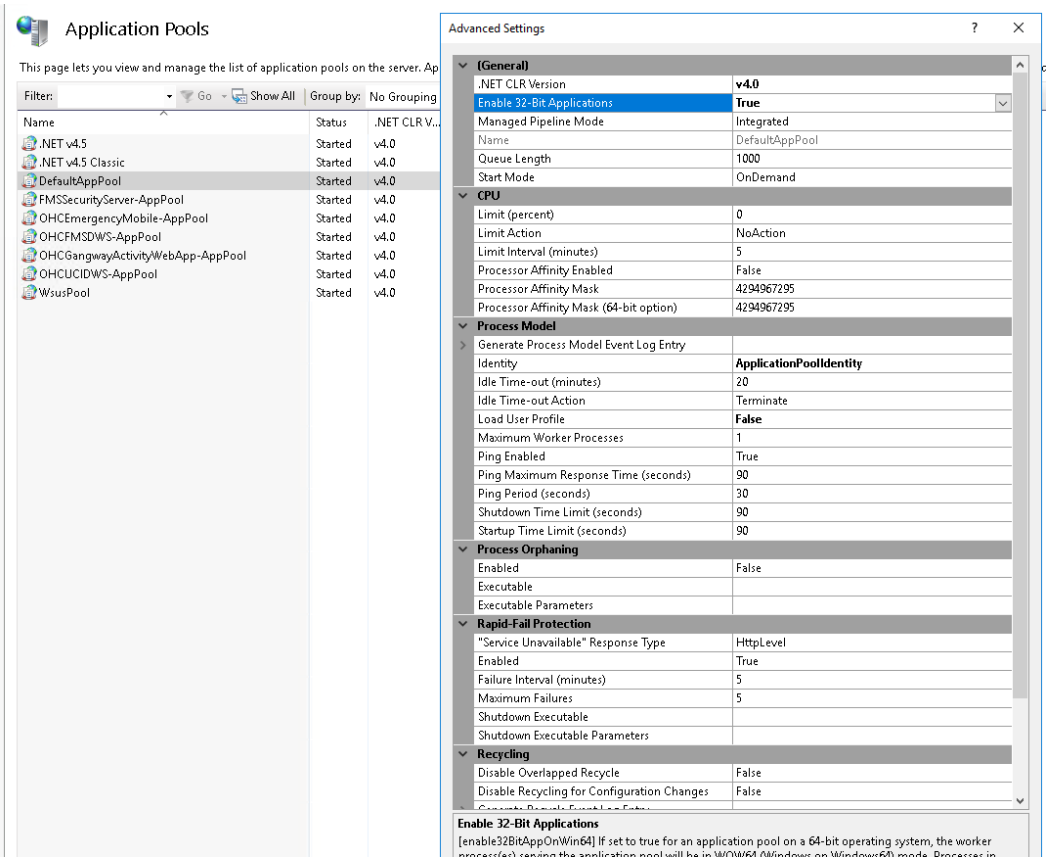


Figure 2-8 - Default App Pool Advanced Settings for Security Server.

Creating a Certificate

To start the IIS server, you need to create a self-signed certificate. To create a self-signed certificate:

1. Run the **.bat** file as administrator. Installation will start with registration of .NET followed by 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.

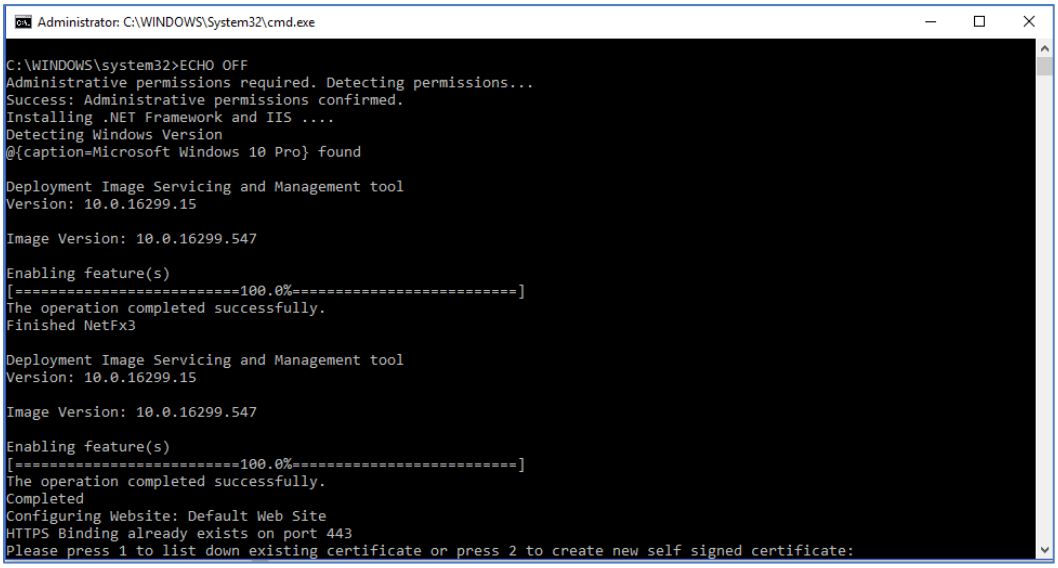


Figure 2-9 - Process to Bind Certificate

2. Process to bind certificate starts. The screen will prompt you to enter 1 to list down existing certificate or press 2 to create new self - signed certificate:
3. Enter 1 to list of all the existing certificates.
4. Write down the subject name to bind the certificate.

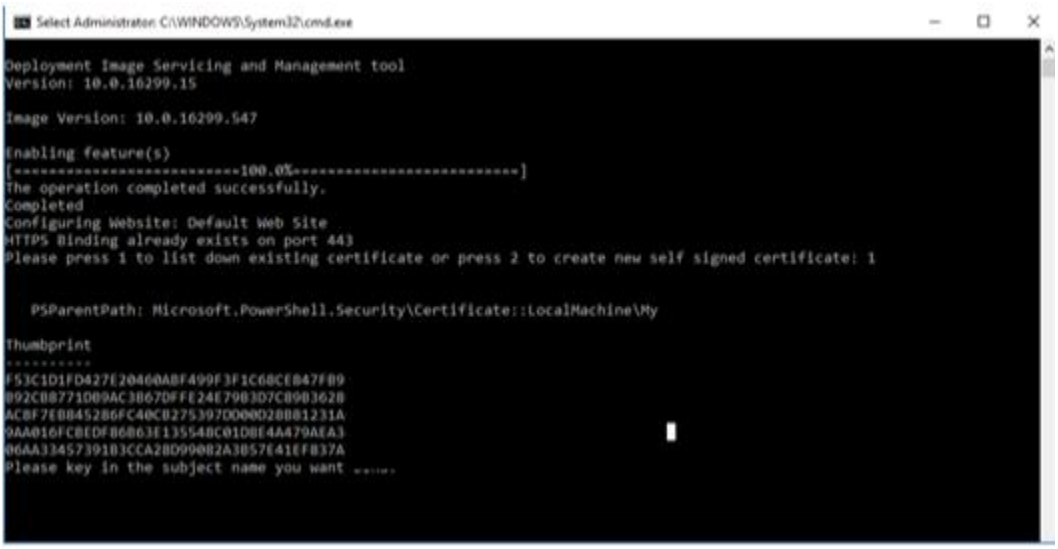


Figure 2-10 - Chosen Certificate Is Binded

5. Chosen certificate is then bind to port 443. IIS is then restarted.

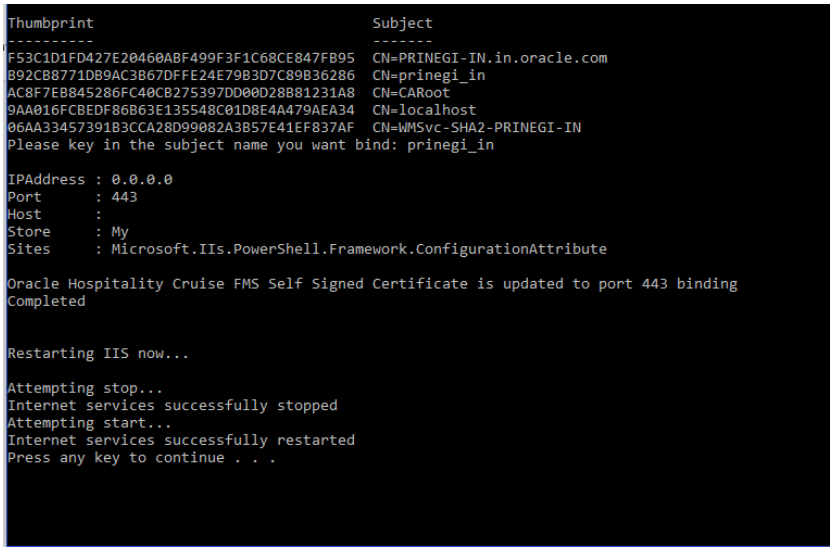


Figure 2-11 - Restarting Internet Information Services (IIS)

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

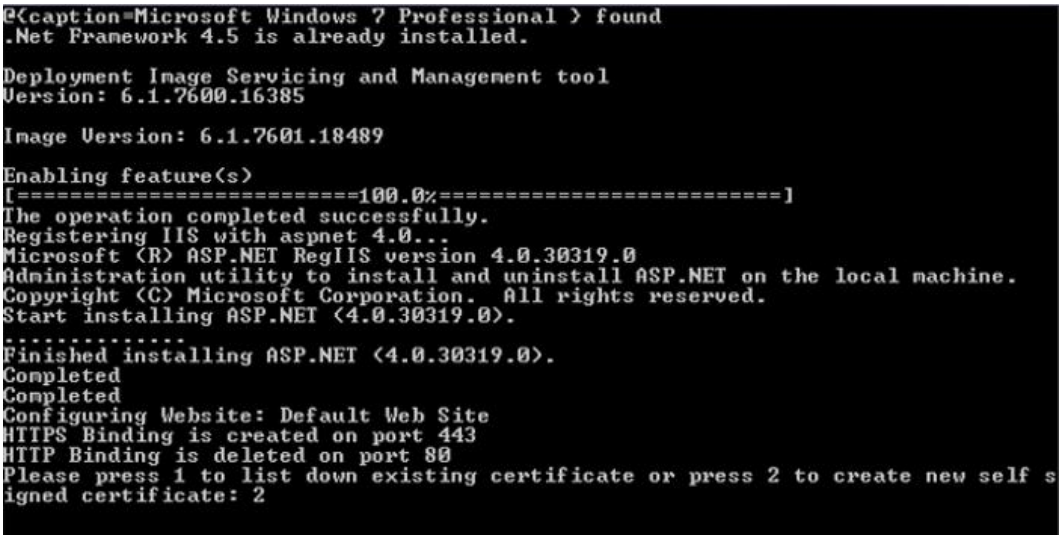


Figure 2-12 - Enter Domain or Internet Protocol (IP) Address

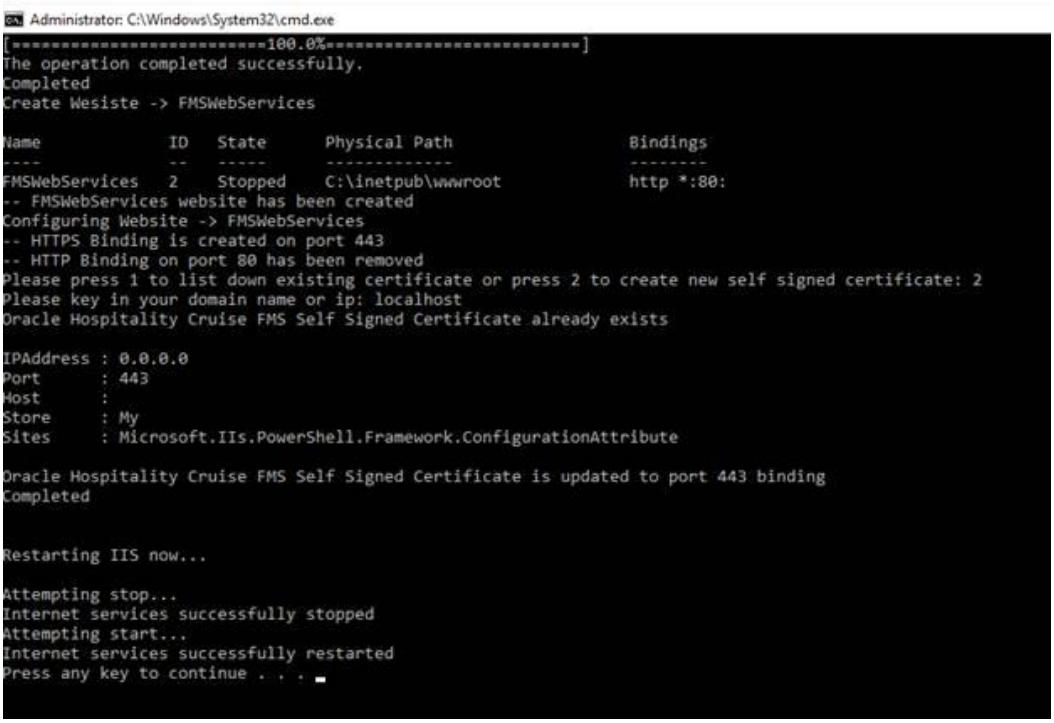


Figure 2-13 - Self-signed Certificate Created

Self-signed certificate is created and is bind to port 443. IIS is then restarted.

Prerequisite for FMS Application Client:

Operating System: Microsoft Windows 10 Enterprise Build 1607 (x64, Bare OS)

RAM: 16GB, Hard Disk Size: 512GB

Oracle Database version: Oracle 11g or Oracle 12c

This guide assumes that you have installed and configured the following elements on the Fleet Management System (FMS) application server:

- Microsoft Windows Server 2016
- Internet Explorer 8.0 and higher
- Internet Information Services (IIS) with the IIS v6 Management Compatibility services.

The following components come bundled in the FMS setup:

- Crystal Reports Runtime engine 32-bit
- .NET Framework 4.5
- A dedicated Client PC installed with Oracle Full Client to run the DB upgrade scripts
- Preinstalled Oracle Data Access Component (ODAC) for PC running FMS applications ODTwithODAC112030
- An administrator user account for Microsoft Windows

Upgrading the Software

The installation requires you to run the installation to have Administrator privileges.

1. Before you begin, ensure these features are turned on and the required files are available.
2. Download the latest FMS patch from Oracle Official Website.
3. Uninstall any previous FMS applications/interfaces that you need to upgrade to FMS 9.x.

Updating the Database

Before you start the upgrade for FMS:

1. Execute the DB scripts using FMS DB Updater from My Oracle Support (MOS) site, number 28841879 for updating the database.
2. Take a backup of "Settings.xml" and "Configsettings.xml" before uninstalling.
   - *Upgrade shore-side FMS Sender/Receiver to 8.2.2.1006 if current version is older. (Older versions can't be upgraded directly to 8.2.2.1007).*
   - *Upgrade shipboard FMS Sender/Receiver to 8.2.2.1006 if current version is older. (Older versions can't be upgraded directly to 8.2.2.1007).*
   - *Upgrade ODAC v11.2.2 to 11.2.3.0 on FMS Sender/Receiver machine(s) shore side*
   - *Upgrade shore-side Receiver/Sender to 8.2.2.1007*
   - *Upgrade ODAC v11.2.2 to 11.2.3.0 on FMS Sender/Receiver machine(s) shipside*
   - *Upgrade ALL Ships Receiver/Sender to 8.2.2.1007 (should be done ship by ship, not big-bang fleet-wide*

3 Pre-Installation Task

Prior to upgrading FMS, 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.*

Make sure the data transfer scripts (FMS_TRANSFER_XXXXXX.sql) are executed on ship DB

4 Uninstalling Fleet Management Component or Add-On

This section describes the Fleet Management Component or Add-On uninstallation process.

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. The uninstallation begins immediately.
3. Go to *C:\Control Panel\All Control Panel Items\Programs and Features* to confirm the Component or Add-On was uninstalled successfully. If the system does not have the Fleet Management Component or Add-On installed, proceed with the next phase.

> **Note**: If the Component or Add-on was already installed and an attempt is made to install the same Component or Add-on, the installation screen shows the Component or Add-on being uninstalled and then reinstalled.

5 Performing a Secure FMS Installation

The following section describes the Fleet Management Component or the Add-On installation process.

1. Right-click the **OHCFM_Suite_9_0_0_0_0.zip** file, and then select **Extract Here**

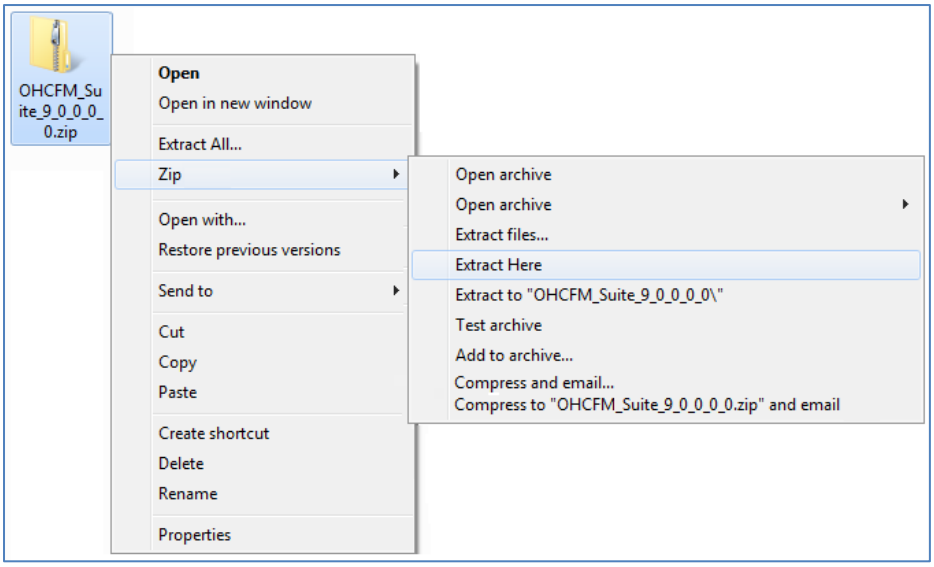


Figure 5-1- File Extraction

2. Open the **OHCFM_Suite_9_0_0_0_0** folder, and then right-click the setup icon. Select **Open/Run as administrator** to install the OHCFM application.

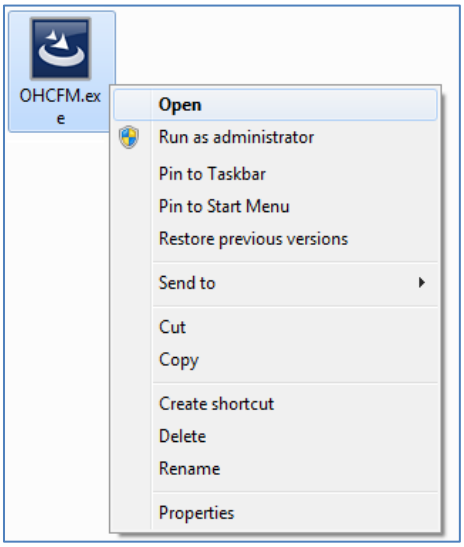


Figure 5-2 – OHCFM Application Installation

3. On the Oracle Welcome screen, click **Next** to continue.

Figure 5-3 – Oracle Welcome Screen

4. 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.

Figure 5-4 – License Agreement

5. Select the required Component or Add-On prerequisites, and then click **Install**.

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**. Installation of the selected prerequisites and Components or Add-Ons should proceed.
3. Click **Finish** to exit the installation process.

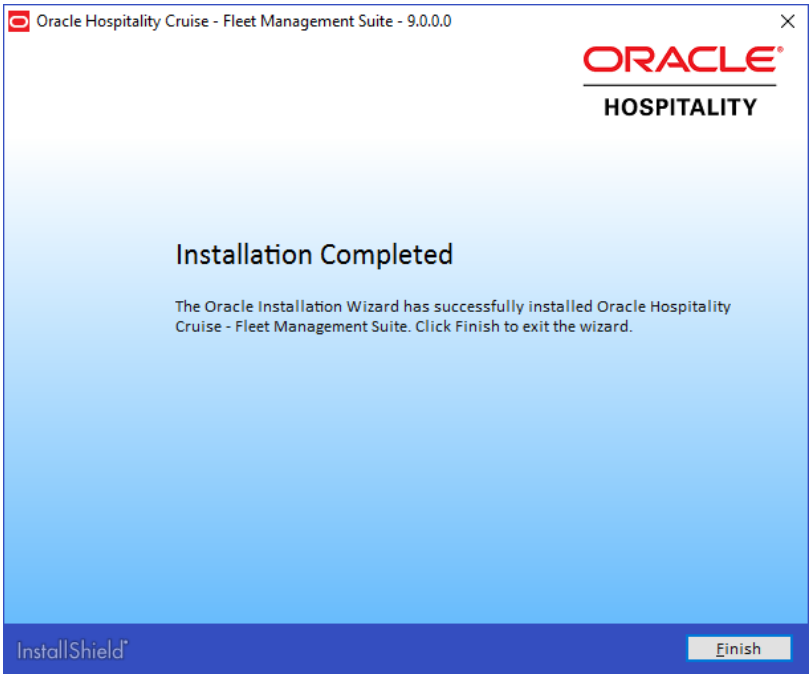


Figure 5-5 – Installation Completed

Post-installation Notes

After completing the installation of Fleet Management:

1. Navigate to *C:\Program Files (x86)\Oracle Hospitality Cruise\OHC FMS* or the directory you specified during installation.
2. Add the ServiceURL information to each Component or Add-On exe.Config file. See example below for ServiceUrl:

```
<appSettings>
   <add key="FidelioBkPassword" value="" />
   <add key="KEKKey" value="" />
   <add key="ServiceUrl" value=" https://<machine_name>/FMSSecurityServer/FCTransactionsService.asmx" />
</appSettings>
```

6 Performing FMS Upgrade

You can perform a custom upgrade or a typical upgrade. A custom installation allows you to exclude the products that you do not need.

Before you start the upgrade, refer to the Prerequisites section.

Upgrading to FMS 9.0

Refer to FMS Upgrade Plan section for details of upgrade.

First step is to upgrade FMS Sender/Receiver fleet-wide to latest FMS8 Sender/Receiver.

1. Upgrade FMS 8.x Server DB from 11g to 12.2c
2. Setup shore side FMS IIS Security Server
   - The customer has to source one SSL certificate for the Security Server
   - With FMS 9, the Ship-side Sender/Receiver will require the FMS Security Server to be installed on the ship's IIS server. The FMS Security server uses the FidelioBK schema and so even if Shipboard Property Management System (SPMS) does not use it with version 8, it should not be removed.
3. Upgrade FMS applications from 8.x to 9.x ((Data Viewer/Corporate Access Module (CAM), ERS, ResOnline (ROL), Corporate Data Transfer Interface (CDTI), Web-Services, Universal Check In (FCUCI))

Changing the Database Password

The next step is to change the schema password of one or all the schemas using DB password Tool. The tool will ensure that the password is a new one and is rotated frequently. One needs to know the System User (SYS) login credentials to use this tool.

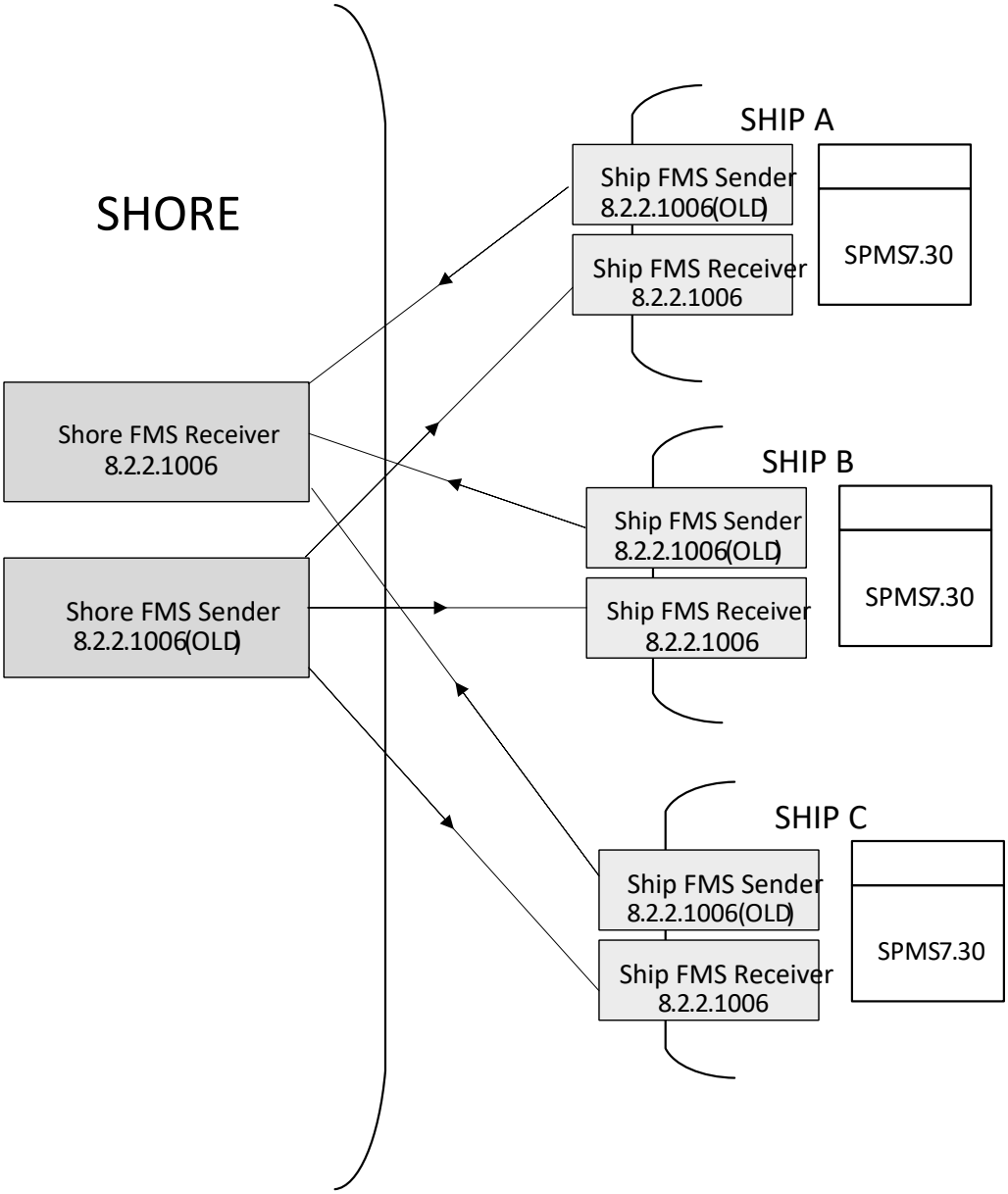
Refer the section on Database Schema Password Manager in Hospitality Cruise Fleet Management User Guide

1. Run **Encryption Manager.**

   If there is any business need that would require stored encrypted data to be viewed at any time by users via the application, then this tool should be run at the background as it will take time depending on the volume of data.

   Refer the section on Encryption Manager (EM) in Hospitality Cruise Fleet Management User Guide

7 FMS Upgrade Plan



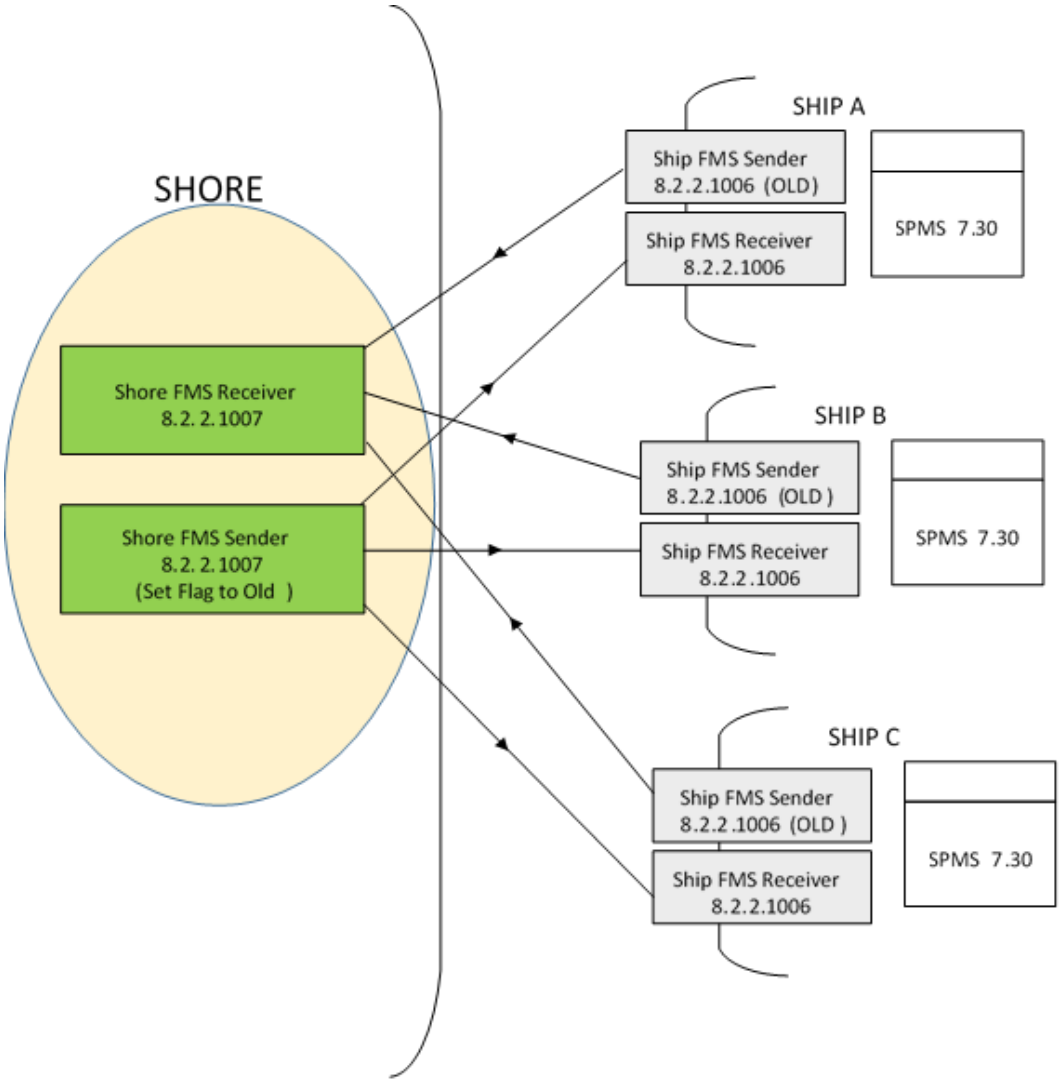
CURRENT STATE – BEFORE ANY UPGRADE

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

- Step 1 must be completed before proceeding to Step 2, 3 and 4.
- Steps 2, 3 and 4 can be done in any order for the various ships and does not need to be at the same time.
- Step 5 can only be done after all steps from 1 to 4 are completed.
- Step 6 can only be done after Step 5 is completed.

- Steps 7, 8 and 9 can only be done after Step 6 is completed.
- Steps 7, 8 and 9 can be done in any order for the various ships and does not need to be at the same time.
- The file APP.CONFIG for the Sender would be named as **FMSSender.exe.Config** in the application's folder.

Step 1

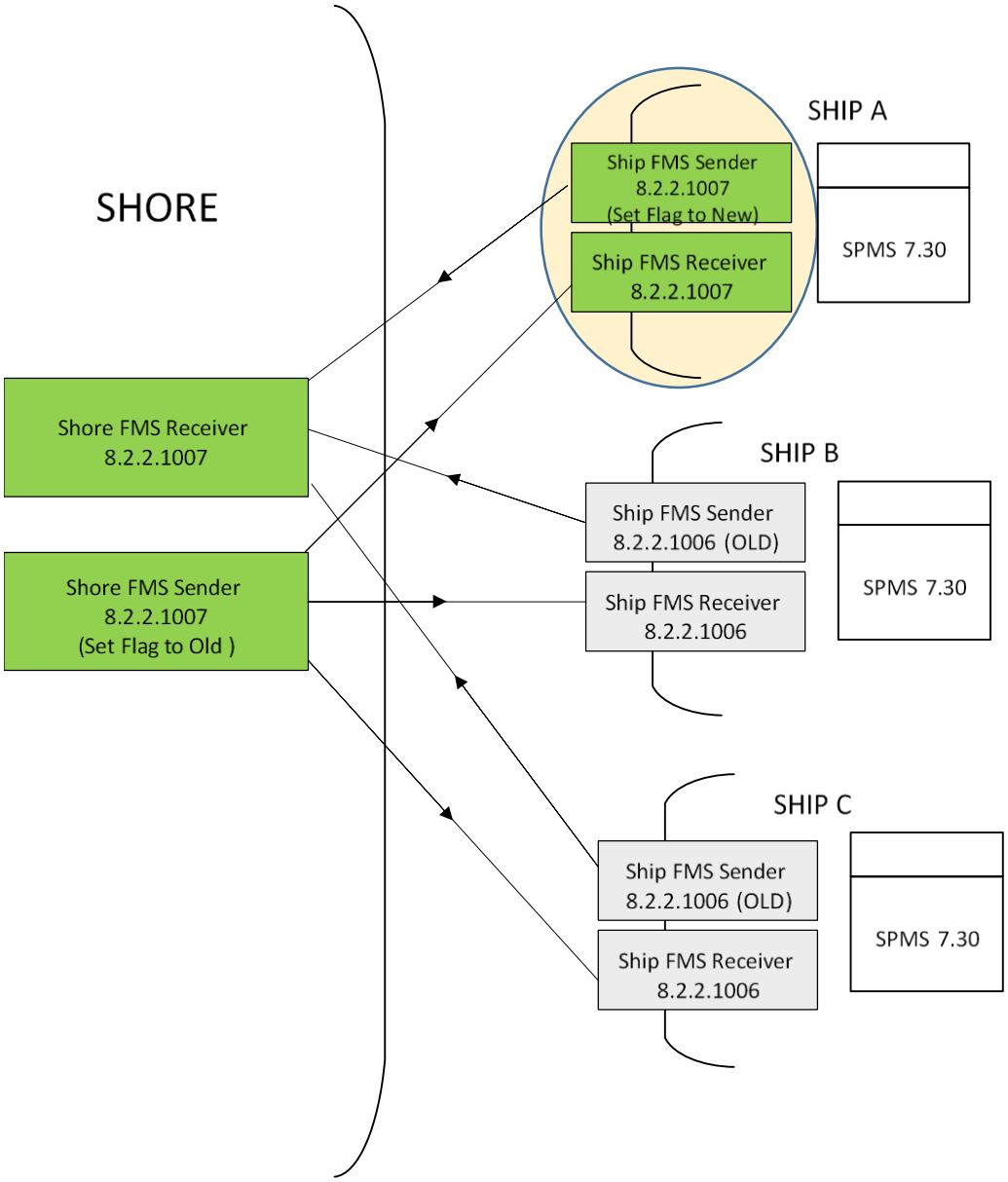


- Install version 8.2.2.1007 Sender & Receiver shore-side to replace the old Sender & Receivers.
- In the shore-side Sender's **FMSSender.exe.Config** file, set the Compression Flag to Old (Case Insensitive).

```
app.config
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

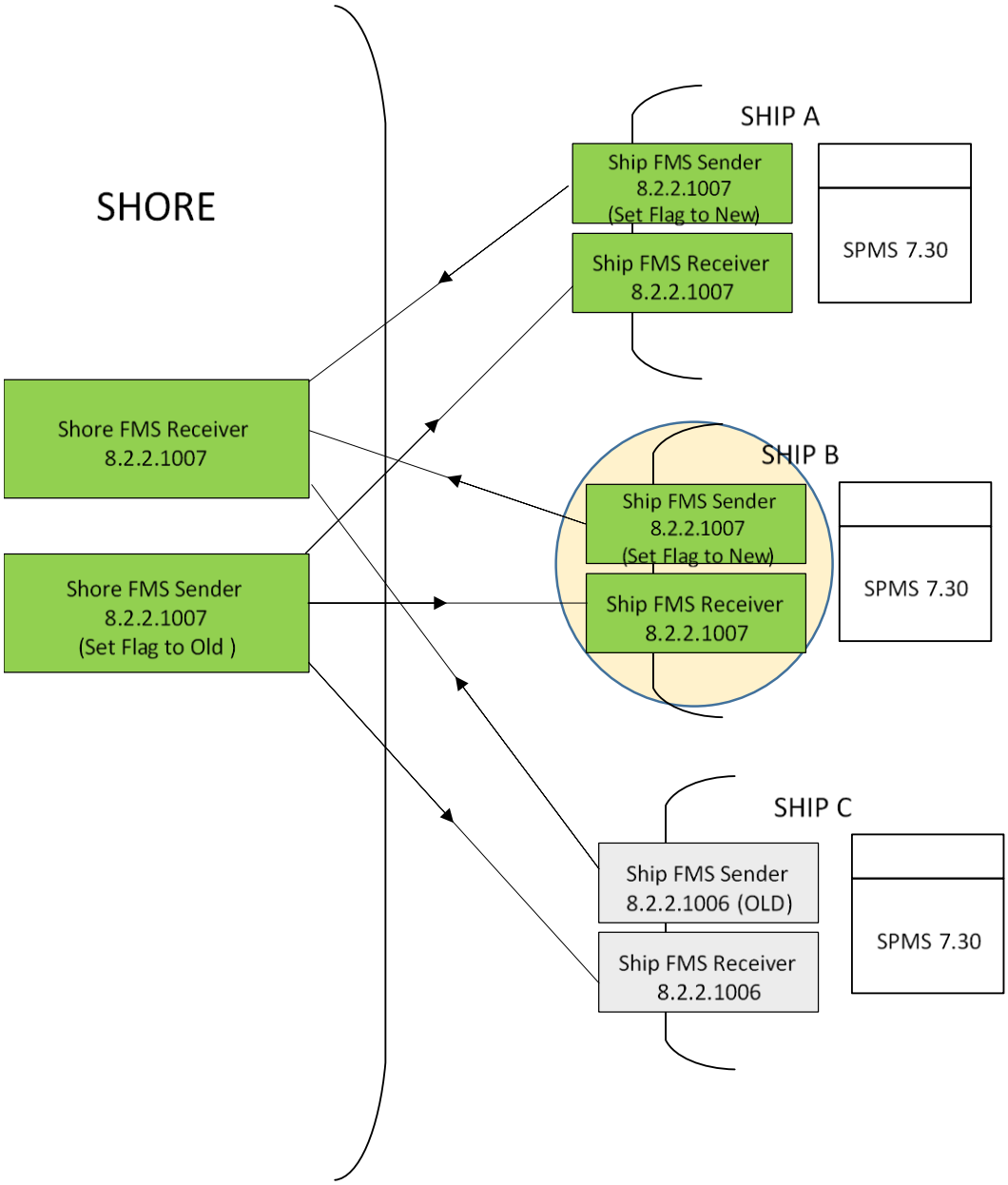
Step 2



- Install version 8.2.2.1007 Sender & Receiver on Ship A to replace the old Sender & Receivers.

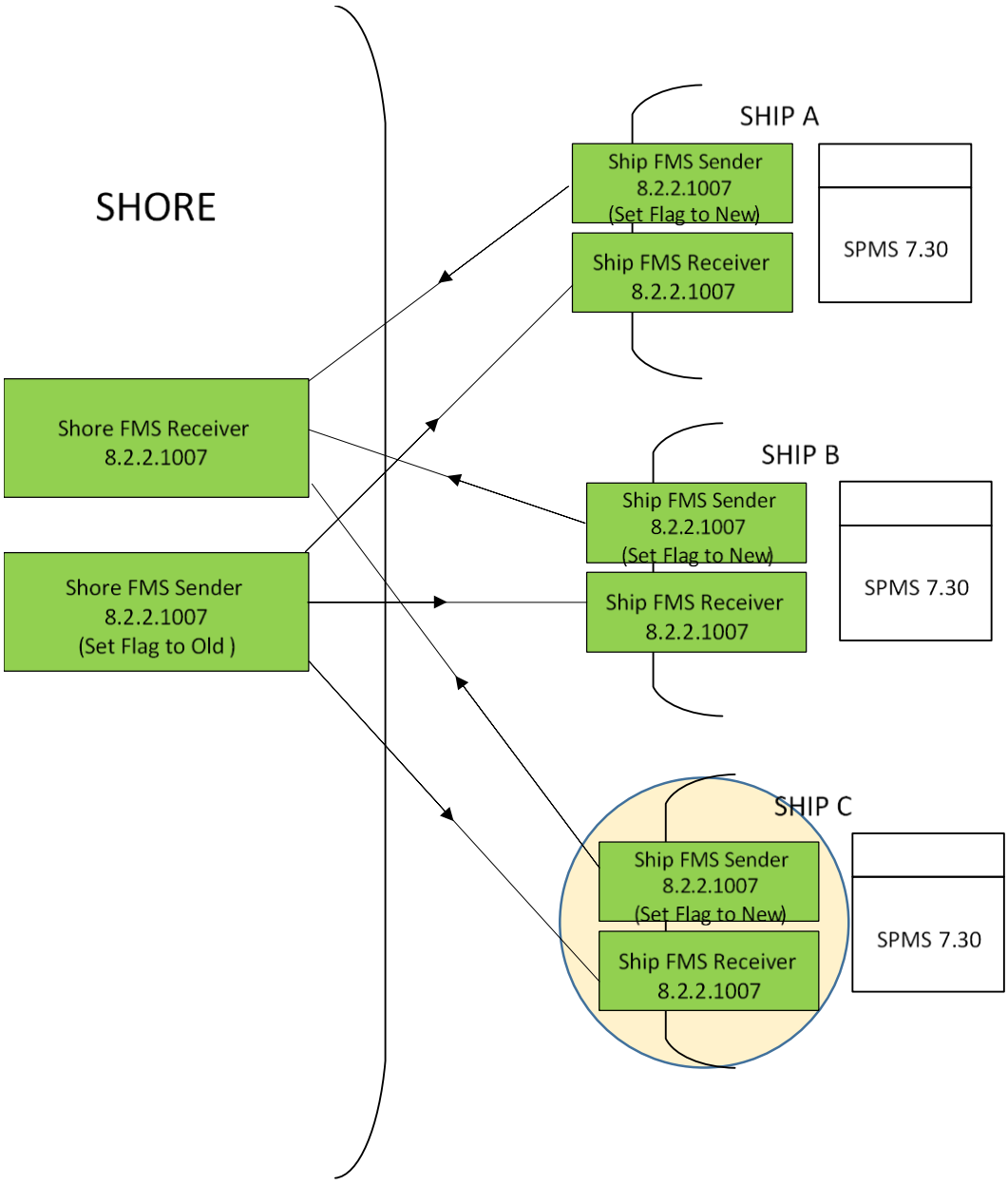
- In Ship A Sender s **APP.CONFIG** file, set the **Compression Flag** to New (Case Insensitive).

Step 3



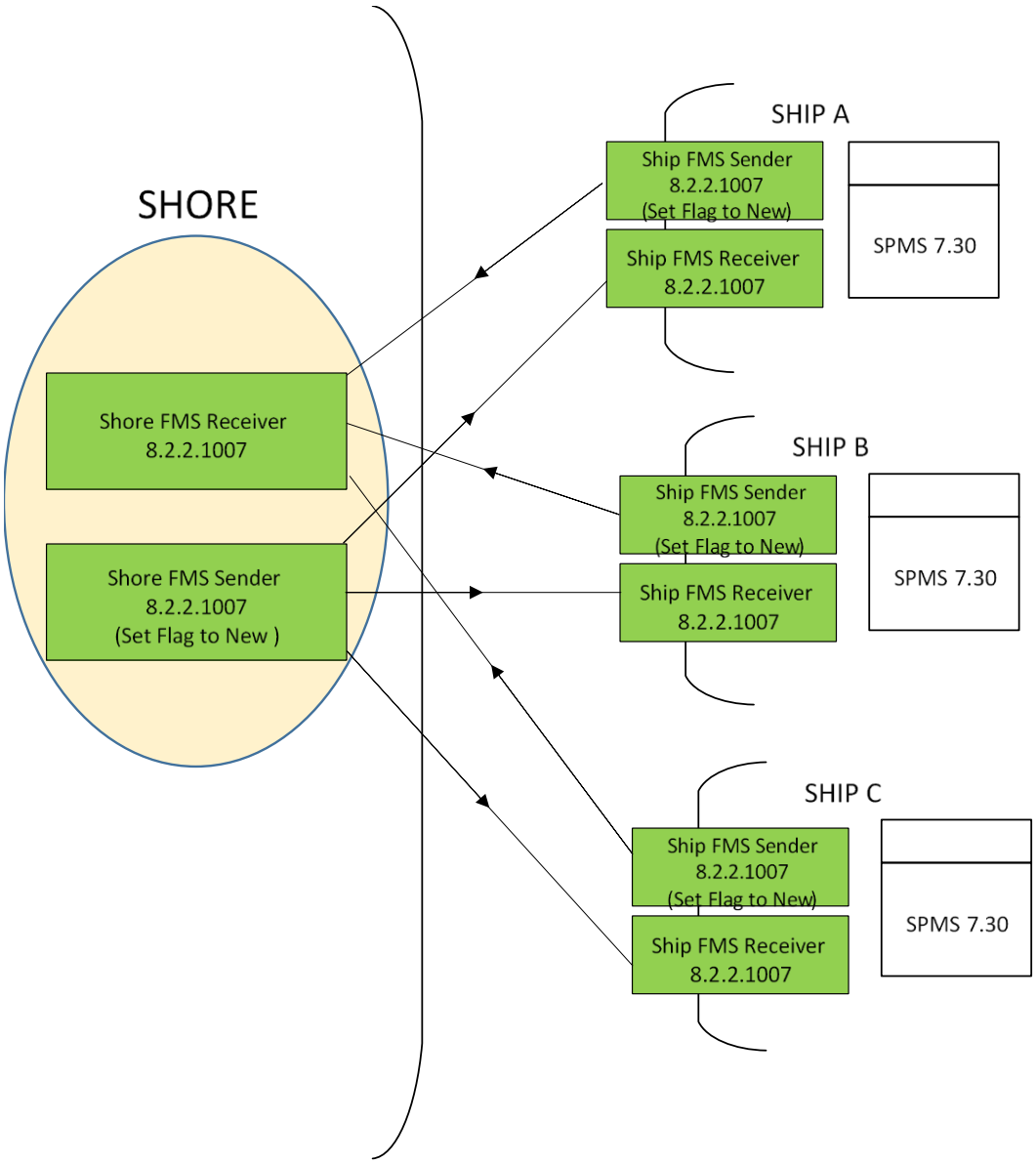
- Install version 8.2.2.1007 Sender & Receiver on Ship B to replace the old Sender & Receivers.
- In Ship B Sender's **FMSSender.exe.Config** file, set the **Compression Flag** to New (Case Insensitive).

Step 4



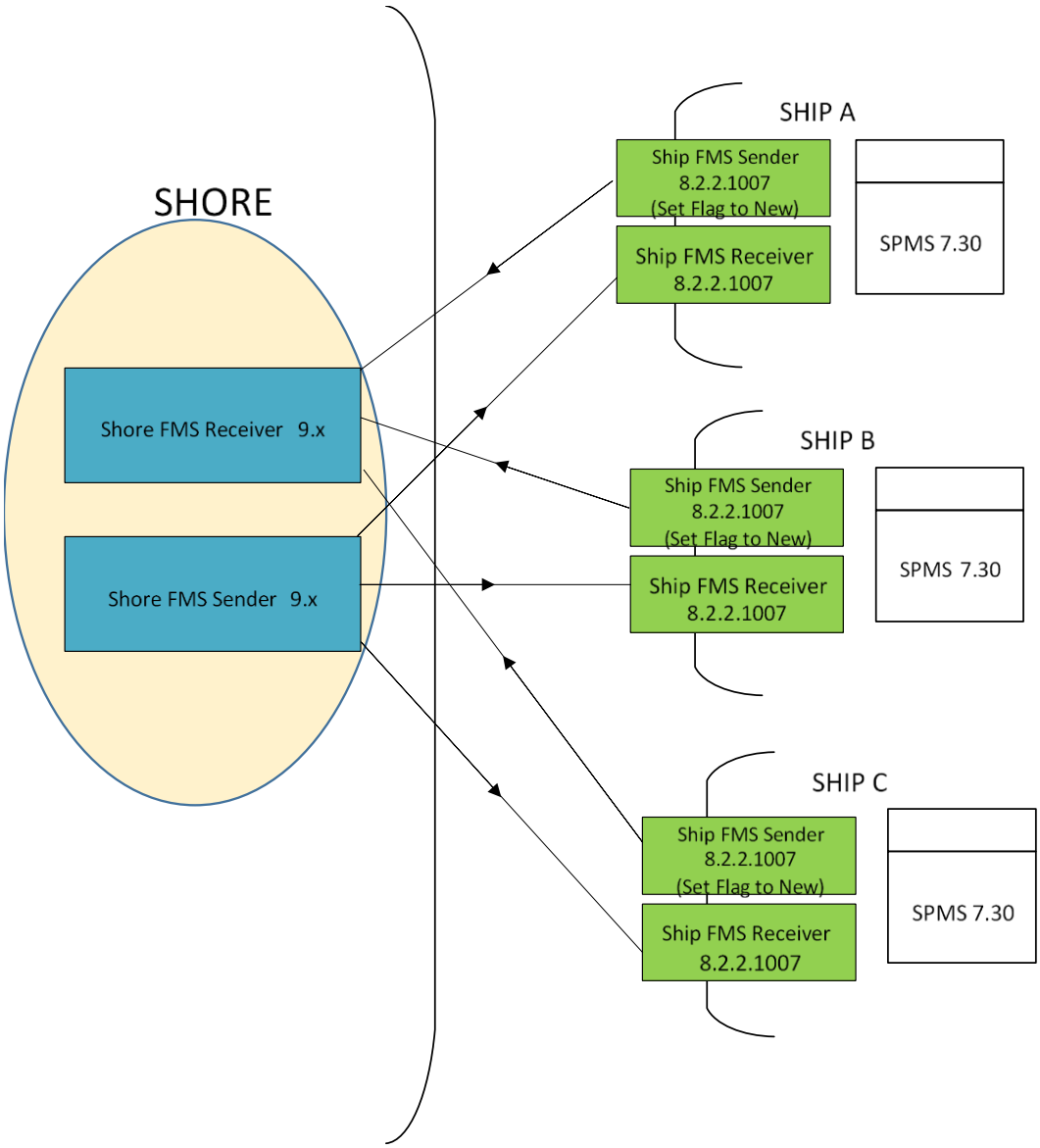
- Install version 8.2.2.1007 Sender & Receiver on Ship C to replace the old Sender & Receivers.
- In Ship C Sender's **FMSSender.exe.Config** file, set the Compression Flag to New (Case Insensitive).

Step 5



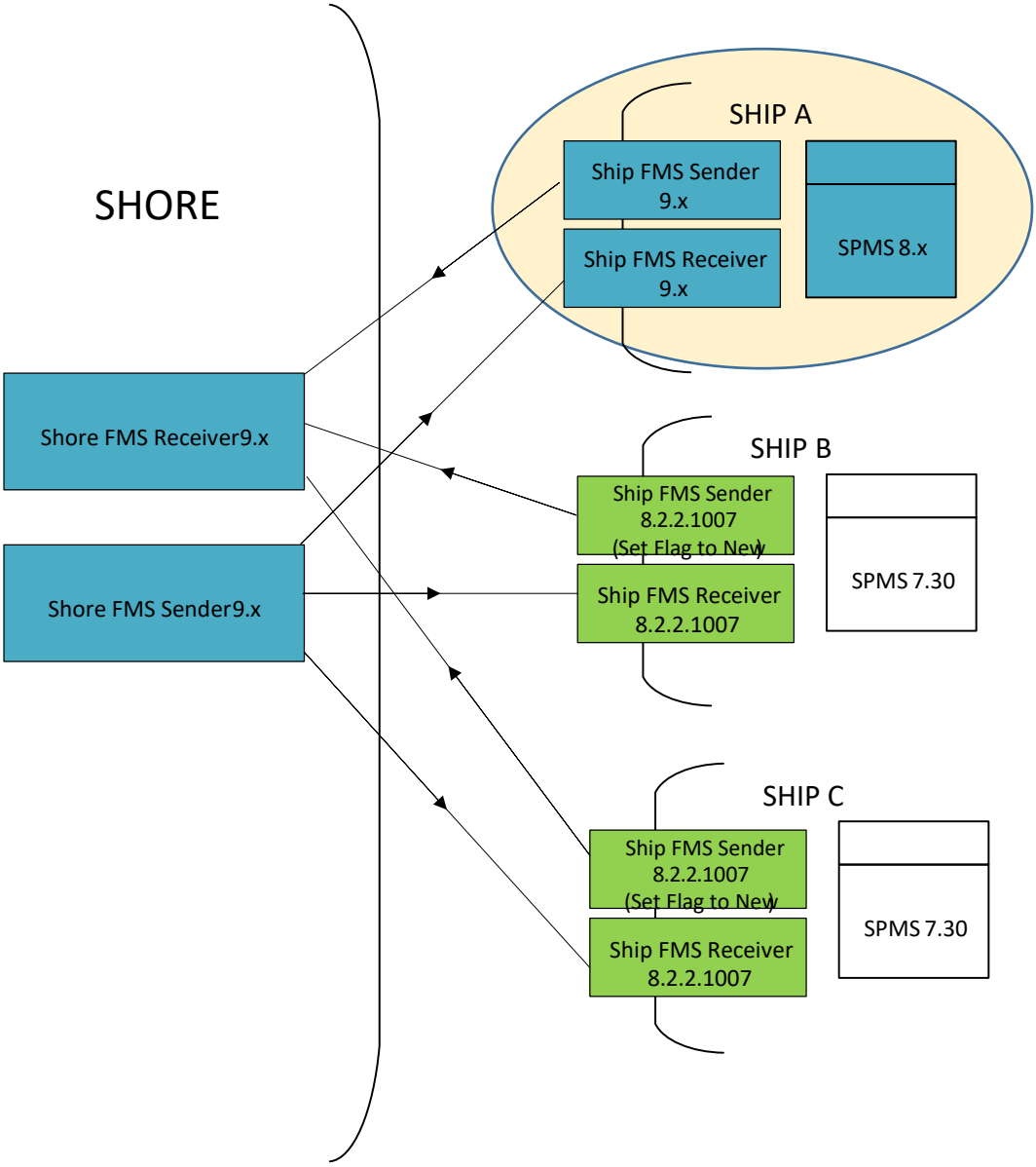
- In the shore-side Sender's **FMSSender.exe.Config** file, set the Compression Flag to New (Case Insensitive) and re-start the Sender.
- This step completes the upgrade process to 8.2.2.1007 across the fleet.

Step 6



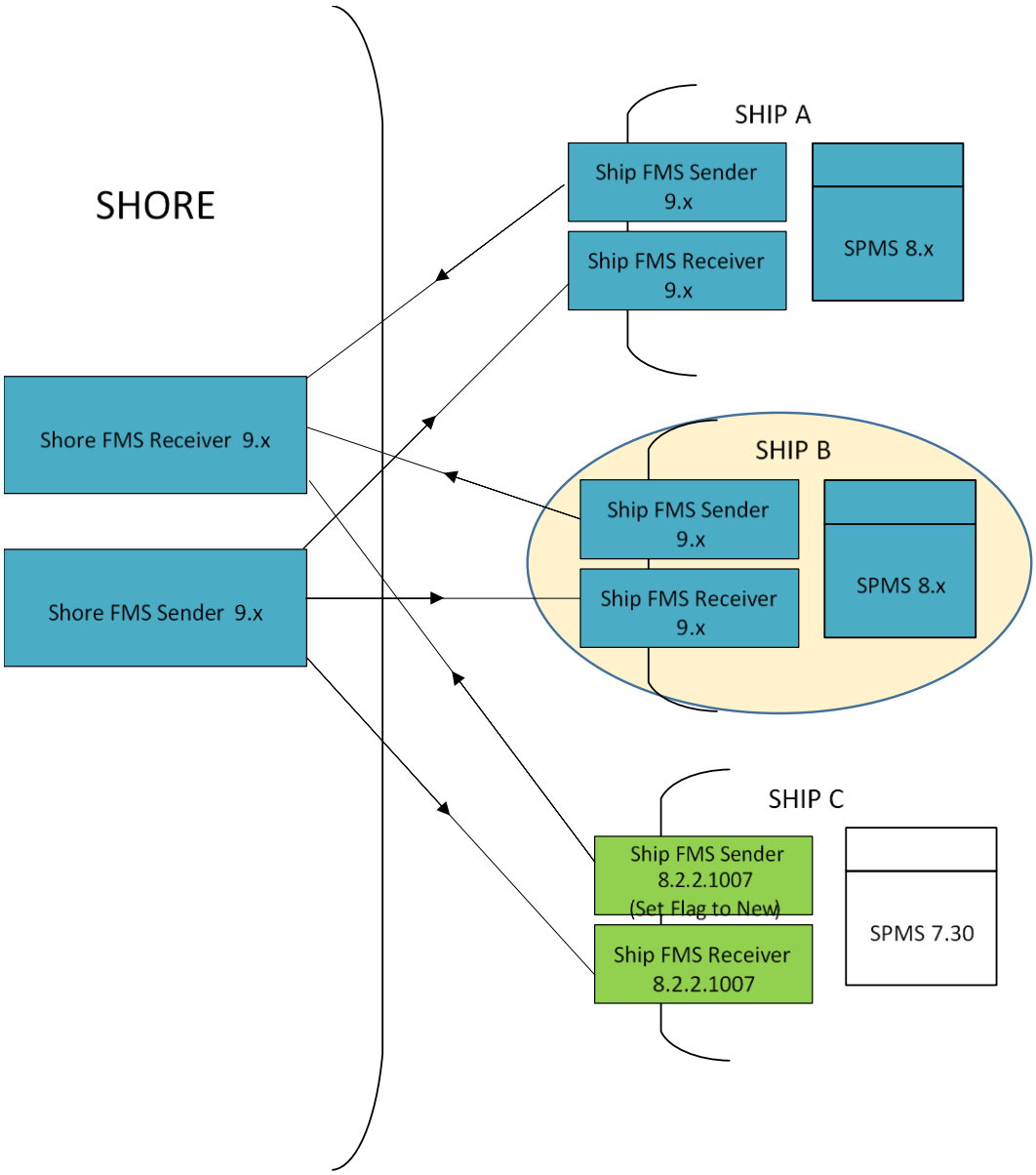
- Before replacing shore-side Sender and Receiver to 9.x, execute the FMS Encryption Manager scripts - (FCONSOL_FMSEncryptionManager.sql) released with 9.0.9.0.
- Upgrade FMS to version 9.x and replace shore-side Sender and Receiver to version 9.x.

Step 7



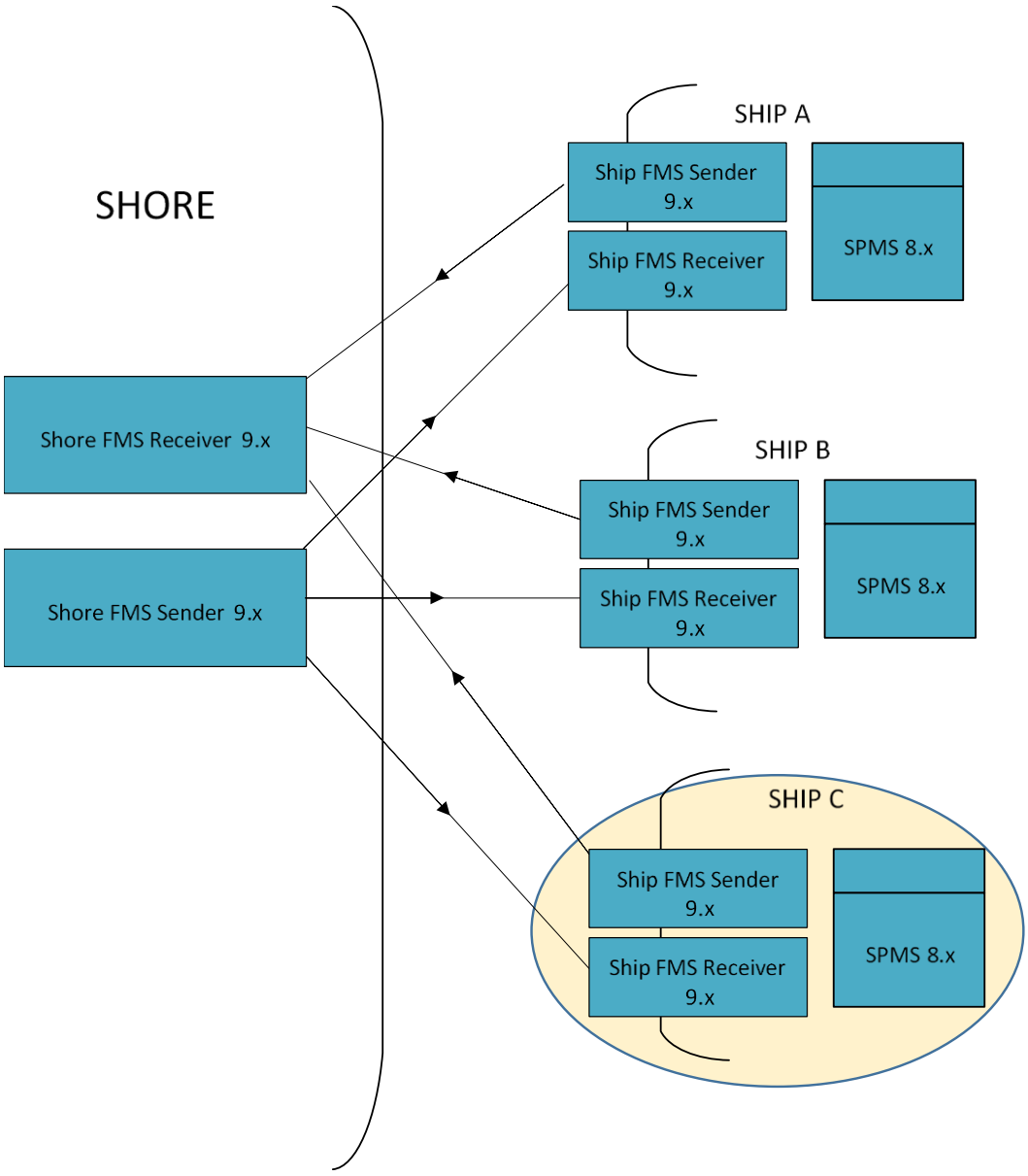
- Upgrade SPMS to version 8.x on Ship A
- Replace Sender and Receiver to version 9.x on Ship A.

Step 8



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

Step 9



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