Oracle Hospitality Cruise Shipboard Property Management System

Installation Guide

Release 23.3
G39309-01
October 2025

Oracle Hospitality Cruise Shipboard Property Management System Installation Guide, Release 23.3

G39309-01

Contents

Preface

1 Getting Started

What You Should Know 1
What You Should Follow 1
Overview of SPMS Components 4
- SPMS Database Server 4
- SPMS Secure Server 5
- SPMS Web Server 5
- SPMS API and Apps Server 6
- SPMS Application Clients 7
- Recommendation for the Installed SPMS Environment 7
  - Typical Configuration 9
  - Alternative Configuration 9
- Installing SPMS Components 11

Where to Download 11

2 Setting Up SPMS .NET Secure Server

SPMS .NET Secure Server Installation Steps 2

3 Setting Up SPMS Database Server

SPMS Database Installation Steps 3

4 Setting Up SPMS .NET Web Server

SPMS .NET Web Server Installation Steps 1

5 Setting Up SPMS Desktop Application Clients

SPMS Desktop Application Clients Installation Steps 1
- Switching between SPMS Application Clients Versions 4

Loading DLLs from SPMS Allowlisted Path 5
Connecting to different SPMS Database using different TNS 6
Uploading SPMS Applications or Libraries to Database 7
Downloading SPMS Applications or Libraries from Database 7
Converting Credit Card Payment from Non-OPI to OPI Tokenization 8
Working with Invalid SPMS Encryption Key 8
Uninstalling SPMS Application Client 9

6 Setting Up SPMS QCI Offline Operation

Setting Up QCI Shore Database and QCI Secure Server 1
Setting Up QCI Shore SPMS Application Client 2
Setting Up Shipside QCI Synchronization Interface 3

7 Installing SPMS REST API/Web Application Server

Preparing the Java Environment 1
Step 1: Create the Java Keystore for SPMS API/Apps Server 2
Generate a new Java Keystore using Java Keytool 3
Generate a Certificate Signing Request (CSR) using Java Keytool 3
Importing SSL/TLS Certificate to the Keystore 4
Step 2: Create the Key Pair for SPMS API Authentication 4
Generating a new Key Pair using JSON Web Key Generator 5
Step 3: Install Oracle Hospitality Cruise Property Management 6
Installing Oracle Hospitality Cruise Property Management 6
Modifying / Uninstalling Oracle Hospitality Cruise Property Management 11
Upgrading Oracle Hospitality Cruise Property Management 12

8 Verifying SPMS Setup

A Appendix

Oracle Database Client and ODAC Installation A-1
Definition of SPMS Seed Database A-2
General Troubleshooting Steps A-2
Common Errors in SPMS Database Installation A-2
Common Errors in SPMS .NET Web Server Installation A-4
Common Errors in SPMS Desktop Application Client Installation A-7
Common Errors in Cruise Property Management Installation - InstallAnywhere A-9
Common Errors in SPMS Mustering Web Application Installation A-10
Common Errors in SPMS REST API/Web Application A-10

Preface

This document provides instructions on how to install the Oracle Hospitality Cruise Shipboard Property Management System (SPMS).

Audience

This document is for technical personnel, programmers, installers, application specialist, and users of SPMS.

Customer Support

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

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

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

Documentation

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

Revision History

Date	Description of Change
October 2025	Initial publication.

1

Getting Started

The following sections provide the information you should know before you install Oracle Hospitality Cruise Shipboard Property Management System (SPMS).

What You Should Know

General Knowledge

- Have an operational understanding of Personal Computers (PC).
- Understand the basic network concepts.

Operating System

- Have working knowledge of Microsoft Windows OS and its user interface (UI).
- Have working experience with Microsoft Windows Administrative privilege.
- Have working experience with Microsoft Windows Server OS, especially Windows Server 2016 or newer version of Windows Server OS.

Database Management System

- Have working experience with the Relational Database Management System (RDBMS), particularly Oracle Database 19c.

SPMS Installation

- You can only install SPMS to local drives. Installation of SPMS on a mapped network drive is not supported.
- Before you perform any SPMS database upgrade or SPMS software installation, you must be logged on with Windows Administrative privileges.

SPMS Integration

- Third-party software providers integrating with SPMS web services must change their application to support the new login method documented in the **OHCWebServices Technical Specifications**, available at the Oracle Help Center for Oracle Hospitality Cruise Shipboard Property Management System Release 23.3
- The SPMS web services login method for SPMS 8.0, 20.X and 23.X are compatible, whereas the SPMS web service login for SPMS 7.30 is different from the rest.

What You Should Follow

Windows Operating System

- Configure the Windows Regional Format to US/UK and set the language to English for all machines installed with SPMS applications to ensure expected SPMS functionality.
- For better security,

- Turn on Data Execution Prevention (DEP) security features.
- Turn off Autoplay and Windows Remote Assistance feature.
- See Microsoft product documentation library at https://technet.microsoft.com/en-us/ for more information and instructions.

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 in SPMS Database is UTF8, 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 table column type in SPMS Database and FMS Database must be the same.
- Additionally, the data type and length of Database table columns for data transfer from/to must be the same between FMS and SPMS.

SPMS Installation

- If a problem occurs during the SPMS application installation, you **cannot** repair or modify SPMS installation features. You **must** reinstall SPMS.
- If you are performing an SPMS database upgrade to this version from SPMS 7.30 or later database, you must perform a database verification and backup tasks for the database before the upgrade process.
- Before you install SPMS software or upgrade the SPMS database, ensure that all other programs and applications on the target machine are closed. If an active program or process is detected, a prompt will notify you to close the active process before it can proceed.
- During the SPMS database upgrade or SPMS installation, follow the instructions carefully on the prompts and do as instructed. If the process is force canceled or closed using methods not as instructed on the prompts, the results can be unpredictable.

Securing SPMS

Update Operating System and Software

- It is extremely important to fully understand and follow closely the guidelines provided in the SPMS Security Guide. We strongly recommend that you read and understand the Security Overview in Section 1 of the *SPMS Security Guide* for your release, available on the Oracle Help Center under Cruise Shipboard Property Management System
- Security patches and quarterly patch releases are common. Therefore, it is the user's responsibility to ensure that the systems used by SPMS are still supported and updated to the latest patch. Always apply security patches on time to prevent and reduce the risk of security vulnerabilities. Check regularly for:
  1. Critical Security Patch of the Operating System.
  2. Critical Security Patch of the Database Management System.

Use of TLS Digital Certificates

- The use of digital certificates is common in today's service-oriented architecture. A digital certificate is especially important in the identification of a system. It is similar to using a government issued identification document to identify an individual. From the SPMS context, the digital certificate is needed to identify the SPMS web services. This is to

prevent an unscrupulous party from impersonating SPMS web services and stealing sensitive information from SPMS. It is recommended that the Digital Certificate used to identify SPMS web services is acquired from a recognized and valid Certification Authority.

- You must install the Secure Sockets Layer (SSL) digital certificate as this is required either on a load balancer or on an IIS Web Server for HTTPS communication to web services. Secure Sockets Layer (SSL) usage on SPMS Security Server is mandatory. Self-signed certificates should be used only if the customer fails to provide a certificate from a Certificate Authority (CA). Refer to the Microsoft product documentation library at https://support.microsoft.com/en-sg/help/324069/how-to-set-up-an-https-service-in-iis for information about the installation of secure certificates.
- The responsibility of acquiring a valid Digital Certificate lies solely with the user. The process does not differ much between different Certification Authorities.
    1. You will need to identify the trusted Certification Authority (CA) that you intend to buy the Digital Certificate from.
    2. Through the CA online purchase portal, you can easily provide the information such as the URL, the purpose of the certificate, and other necessary information to acquire a Digital Certificate.
    3. Alternatively, you can generate a Certificate Signing Request and send it to the CA to be signed.
    4. Regardless of the differences, the purpose remains the same, which is to acquire a Secure Sockets Layer (SSL) compliant digital certificate for the SPMS web services from a recognized and valid Certification Authority.
- The act of generating a self-signed Digital Certificate to identify the SPMS web services is not recommended for the production environment. It increases the risk of an unscrupulous party impersonating the SPMS web services to steal sensitive information. However, it is still possible for SPMS web services to use a self-signed certificate despite the increased security risk, which means you would have to agree to bear the consequences.

Follow Strict Password Policy

- Adhere to the following rules of the system enforced password policy, or whichever is deemed safer when dealing with passwords, regardless of the Database user password, OS user password, or SPMS user password. The Password must be:
    1. At least ten (10) characters long.
    2. A combination of uppercase and lowercase letters, numeric characters, and special characters.
    3. Must NOT be one of the last three passwords used.
- As for the SPMS user passwords, they are configured in the SPMS User Security module. Administrators should adopt a strong password policy after the initial installation of the application and review the policy periodically. Ensure the password adheres to the following strength requirements:
    1. The password must be at least ten (10) characters long.
    2. The password must contain letters, special characters and numbers.
    3. Must not select a password equal to the last three (3) passwords used.
    4. Password change every 90 days.
    5. Password Lockout Minutes is 30 minutes.
    6. Maximum Incorrect Login before lockout is 6.
    7. Idle Minutes before logged out is 15.

8. Idle Minutes before logged out on Launch Panel is 15.

- When logging in for the first time, you are required to change the user password in SPMS, using the above guidelines.

Adopt Least Privilege Security

- When setting up users for the SPMS application, ensure that they are assigned with the minimum privilege level required to perform their job functions.

Overview of SPMS Components

To set up a full SPMS 23.3 environment, the following components are required:

1. SPMS Database Server.
2. SPMS .NET Secure Server.
3. SPMS .NET Web Server.
4. SPMS Desktop Application Clients.
5. SPMS REST API Server.
6. SPMS Web Application Server.

It is important that you know and understand that each of the components listed above is not restricted to one component per machine. Depending on your operation requirements and resource availability, you can select one of the following options:

1. Install all the components in the same machine.
2. Install each component separately in a different machine.
3. Install the components using a combination of both option 1 and option 2.

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 Operating System and Database version.

SPMS Database Server

The SPMS Database Server is the machine that hosts the database of the SPMS applications. It is the core or heart of the SPMS environment. It must be installed with database management software and configured to handle database requests from multiple database clients.

Minimum System Specification

- Operating System:
  - Microsoft Windows Server 2016
- Memory:
  - 8 GB of RAM, and
  - 160 GB of disk space.
- Oracle Database Version:
  - Oracle Database Server 19c
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC

- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and
  - Framework version 4.8 enabled.

SPMS Secure Server

The SPMS Secure Server hosts the web service that manages the user credentials. It is similar to password manager software. In SPMS 7.30, there is no Secure Server. Instead, a separate database schema handles the same responsibility. From SPMS 8.0, 20.X, 23.X, or newer versions, the database schema is replaced by a web service hosted on a web host (SPMS Secure Server) that handles HTTPS requests from multiple clients.

> **Note**
>
> SPMS Secure Server installation files are bundled with the SPMS Transactions Service. Therefore, installing the SPMS Transactions Service also deploys a copy of the SPMS Secure Service.

Minimum System Specification

- Operating System:
  - Microsoft Windows Server 2016
- Memory:
  - 8 GB of RAM, and
  - 160 GB of disk space.
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC
- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft Internet Information Services (IIS):
  - IIS v10 with Management Compatibility Services
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and
  - Framework version 4.8 enabled.

SPMS Web Server

The SPMS Web Server is a web host to the SPMS web services for SPMS applications and integrations. It provides SOAP-based web services to access the SPMS functions. SPMS web services are hosted on Microsoft IIS. Oracle recommends that the web services be secured

with TLS (HTTPS). The SPMS Web Server can host any of the three SPMS web services, or a combination of the SPMS web services, or all of them altogether. The SPMS web services distributed are:

1. OHC SPMS Transactions Service,
2. OHC SPMS Web Services, and
3. OHC SPMS OPI Web APIs.

> **Note**
>
> You can install all the SPMS web services on the same machine or install them separately, depending on the resource availability and operational requirements.

Minimum System Specification

- Operating System:
  - Microsoft Windows Server 2016
- Memory:
  - 8 GB of RAM, and
  - 160 GB of disk space.
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC
- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft Internet Information Services (IIS):
  - IIS v10 with Management Compatibility Services
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and
  - Framework version 4.8 enabled.

SPMS API and Apps Server

The SPMS API & Apps Server is a web host to the Cruise Property Management System web apps and REST APIs.

Minimum System Specification

- Operating System:
  - Microsoft Windows Server 2019
- Memory:
  - 16 GB of RAM, and
  - 250 GB of disk space.
- Oracle Database Client Version:

  - Oracle Database 32-bit Full Client for 19c including the ODAC

SPMS Application Clients

The SPMS Application Clients are service consumers that connect to the SPMS Database Server or SPMS Web Server to perform their intended operation.

Minimum System Specification

- Operating System:
  - Microsoft Windows 11 Standard Edition
- Memory:
  - 8 GB of RAM, and
  - 160 GB of disk space.
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC
- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and
  - Framework version 4.8 enabled.

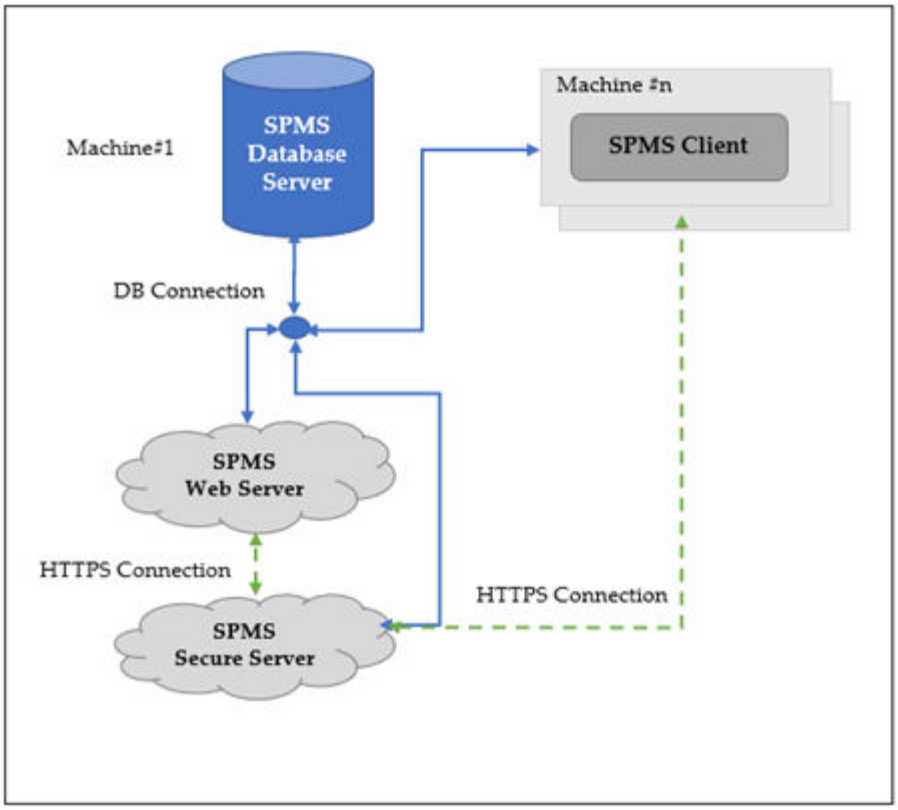
Recommendation for the Installed SPMS Environment

In this section, we suggest some of the possible installed SPMS environments. You are in no way limited by the examples of the installed SPMS environment shown below.

Minimal Configuration

In the configuration shown below, the SPMS Database Server and SPMS Web Server are installed on the same machine. The minimum system specification for this type of configuration will be the combination of both the SPMS Database Server and SPMS Web Server.

Figure 1-1 Minimum SPMS Configuration



Minimum System Specification for Combined Web Server and Database Server

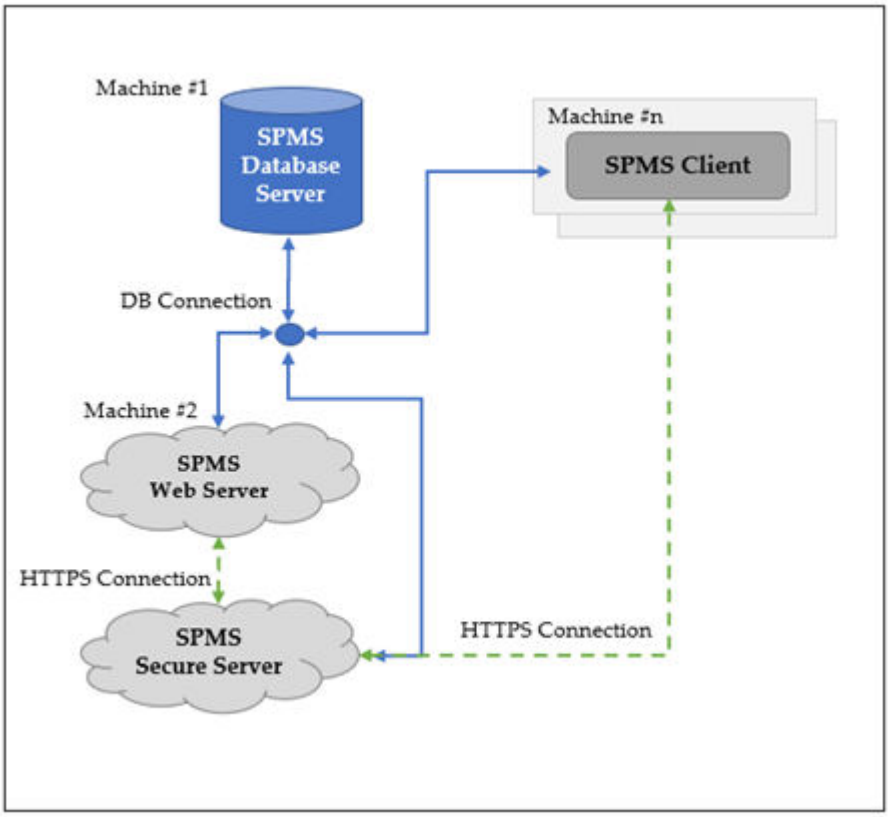
- Operating System:
  - Microsoft Windows Server 2016
- Memory:
  - 16 GB of RAM, and
  - 320 GB of disk space.
- Oracle Database Version:
  - Oracle Database Server 19c
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC
- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft Internet Information Services (IIS):
  - IIS v10 with Management Compatibility Services
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and

– Framework version 4.8 enabled.

Typical Configuration

In the configuration shown below, the SPMS Database Server and SPMS Web Server are installed separately on different machines. The benefit of this configuration is that there is a clear delineation where all the database traffic will be directed to the machine hosting the SPMS Database, and all the web requests will go to the SPMS Web Server. The minimum system specification for this configuration remains the same as recommended in SPMS Database Server, SPMS Secure Server, SPMS Web Server, and SPMS Application Clients.

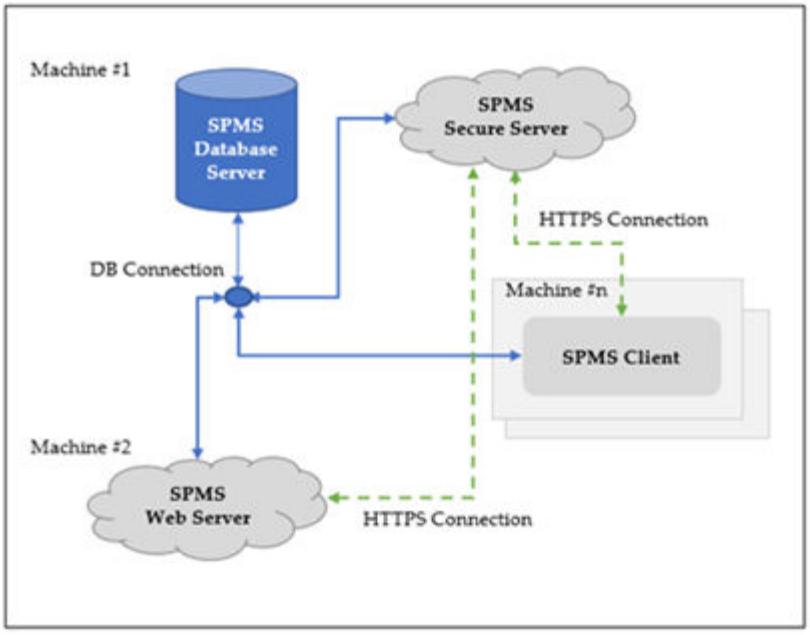
Figure 1-2 Typical SPMS Configuration



Alternative Configuration

In the configuration shown below, the SPMS Database Server and SPMS Web Server are installed separately on different machines. Here, the SPMS Secure Server is installed on the same machine as the SPMS Database. In the older SPMS version, the SPMS Database Server handles all database requests and also manages the secure server responsibilities through the two SPMS Database schemas.

Figure 1-3 Alternative SPMS Configuration



Minimum System Specification for Combined Secure Server and Database Server

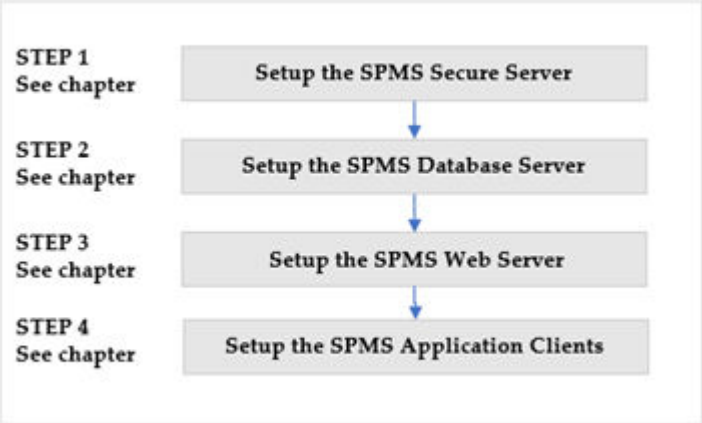
- Operating System:
  - Microsoft Windows Server 2016
- Memory:
  - 8 GB of RAM, and
  - 160 GB of disk space.
- Oracle Database Version:
  - Oracle Database Server 19c
- Oracle Database Client Version:
  - Oracle Database 32-bit Full Client for 19c including the ODAC
- Web Browser:
  - any web browser, visit Oracle Software Web Browser Support Policy.
- Microsoft Internet Information Services (IIS):
  - IIS v10 with Management Compatibility Services
- Microsoft .NET Framework runtime:
  - Framework version 2 enabled,
  - Framework version 3.5 enabled, and
  - Framework version 4.8 enabled.

Installing SPMS Components

As shown in the Recommendation for the Installed SPMS Environment section, the SPMS installation consists of setting up all the components listed below.

1. SPMS Database Server,
2. SPMS Secure Server,
3. SPMS Web Server, and
4. SPMS Application Clients.

Figure 1-4 SPMS Summarized Installation Process Flow



Where to Download

SPMS releases are available at:

1. Oracle Software Delivery Cloud (OSDC).
2. My Oracle Support (MOS).

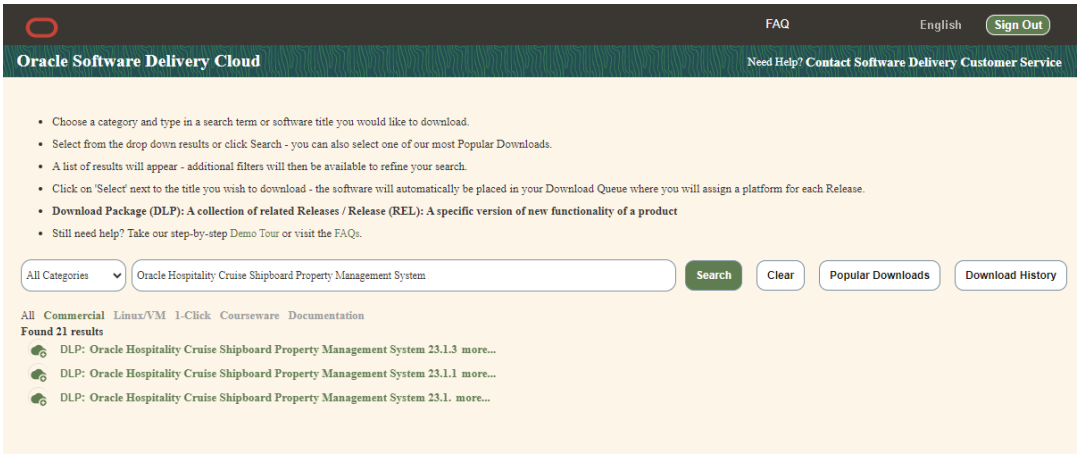
For a Major/Minor release, the first upload is on OSDC. Patch and Hotfix releases are subsequently uploaded to MOS. See My Oracle Support Help for download instructions.

SPMS Installation File

The Initial Release of the SPMS Installation files are distributed in OSDC. Running the SPMS Installation files will install all libraries, dependencies, and the bare minimum required by SPMS applications. Installation does not give you access to all SPMS applications. You need to download and deploy the SPMS package files. Follow the instructions below to download the SPMS Client Installer from Oracle Software Delivery Cloud.

1. Log in to the Oracle Software Delivery Cloud. https://edelivery.oracle.com/osdc/faces/Home.jspx
2. Search for Oracle Hospitality Cruise Shipboard Property Management System. Follow the instructions stipulated on the page to download.

Figure 1-5 Sample Oracle Software Delivery Cloud Download Page

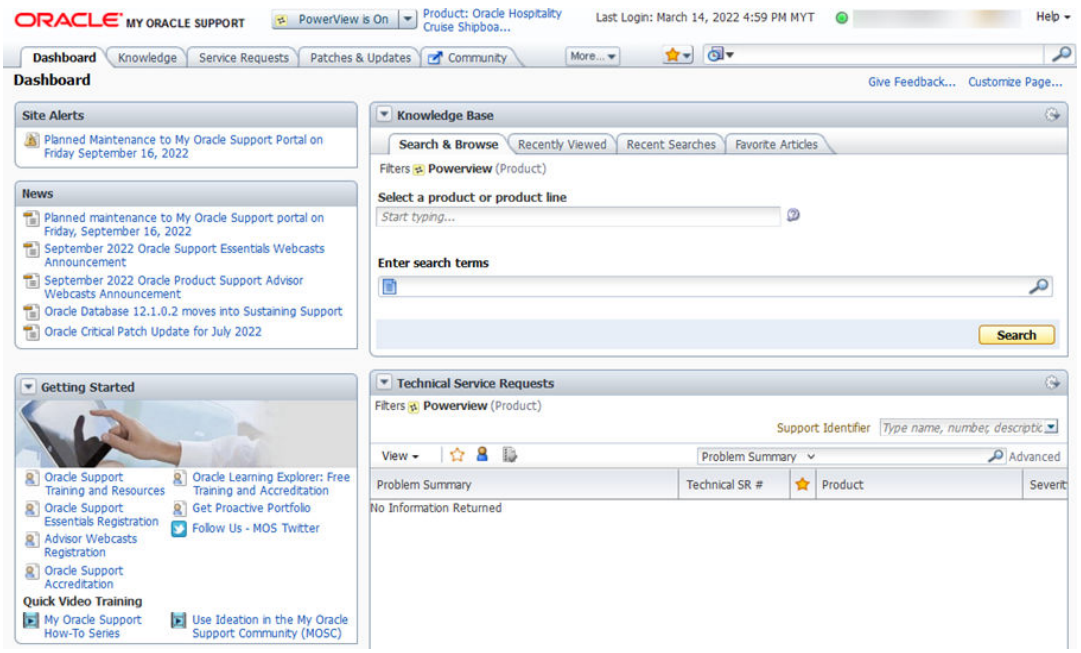


3. Locate the downloaded SPMS Installation package in your download folder.

SPMS Package File

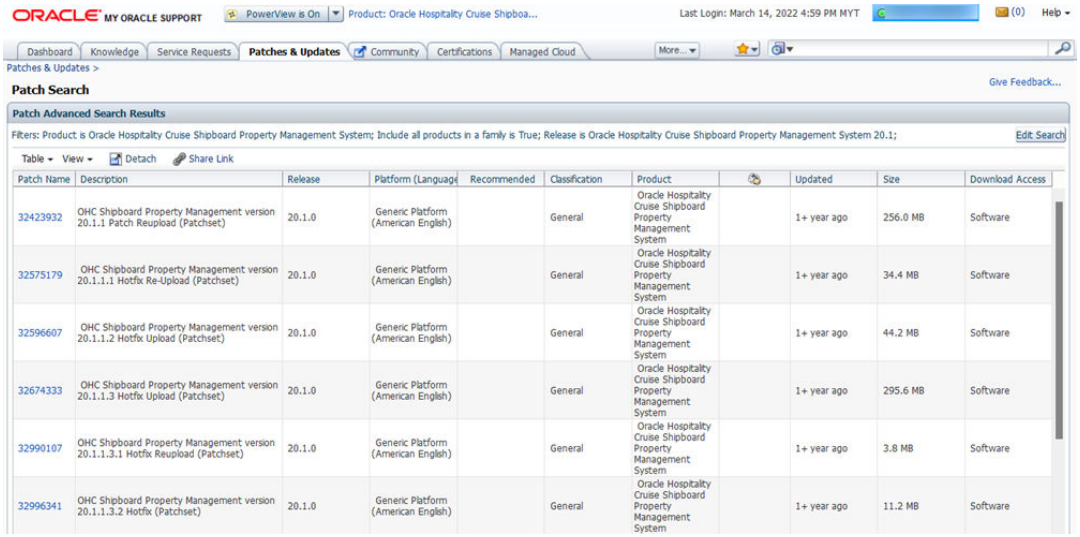
The SPMS Package files distributed in the later Patch and Hotfix releases are uploaded to My Oracle Support (MOS). The SPMS Package file contains programs, libraries, web services, and scripts deployed by SPMS. You can download the SPMS Package from My Oracle Support (MOS) using the instructions below:

1. Log in to My Oracle Support.
2. Upon a successful login, you are redirected to the Dashboard page below:



3. Select the **Patches & Updates** tab. Search for **Oracle Hospitality Cruise Shipboard Property Management System**
4. Select the package version to download.
5. Click **Search** to obtain the patch lists.

Figure 1-6 SPMS Patch List



6. From the result list, select the patch to download.
7. The screen shot below shows the downloaded SPMS Package folder.

2

Setting Up SPMS .NET Secure Server

The SPMS Secure Server is a Microsoft IIS host machine that hosts the Microsoft SOAP based SPMS web service, developed to manage login credentials and encryption keys. It is comparable to a password management application.

To set up the SPMS Secure Server, install the SPMS Secure Service, which is one of the SPMS web services developed using the .NET framework and distributed as part of the SPMS Package.

SPMS .NET Secure Server Prerequisites

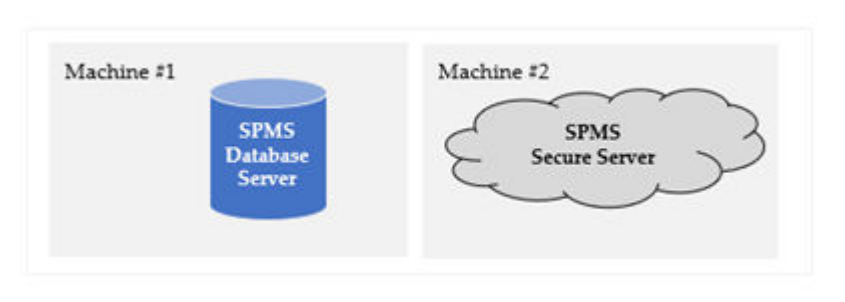
1. Microsoft IIS installed on the target machine.
2. Microsoft .NET Framework 2.0, 3.5, and 4.8 features are enabled on the target machine.
3. Oracle 19c Database client with ODAC is installed on the target machine. See topic Oracle Database Client and ODAC Installation.
4. SPMS Package is downloaded and available in the target machine. See topic SPMS Package File for download instructions.
5. SPMS Application Client installed. See topic Setting Up SPMS Desktop Application Clients.

Important

Before proceeding, it is important to know where you intend to set up the SPMS Secure Server. See topic Recommendation for the Installed SPMS Environment for some examples of SPMS Environment configurations. You can choose to install SPMS Secure Server on the same machine as in the SPMS Database Server or a separate machine.

Figure 2-1 SPMS DB Server and SPMS Secure Server on the same machine

Figure 2-2 SPMS DB Server and SPMS Secure Server on different machine



- The SPMS Secure Server must be reachable by all SPMS Application Clients and the SPMS Web Server as it manages the Database user credentials, which require an established SPMS-Database connection.
- The SPMS Secure Server must be able to connect to the SPMS Database as it will need to verify the Database connection before it can store the Database user credentials.

SPMS .NET Secure Server Installation Steps

To set up SPMS Secure Server, follow the steps in the order shown below:

1. See topic Installing SPMS Secure Service
2. See topic Verifying Hosting of SPMS Secure Service
3. See topic Setting Up SPMS Secure Service Database Connection

Installing SPMS Secure Service

The SPMS Secure Server hosts the SPMS Secure Service. As SPMS Secure Service is distributed with the SPMS web services of the SPMS Package, the steps to install SPMS Secure Service are similar to the SPMS web services installation. See Installing SPMS Web Services for the step-by-step installation instructions.

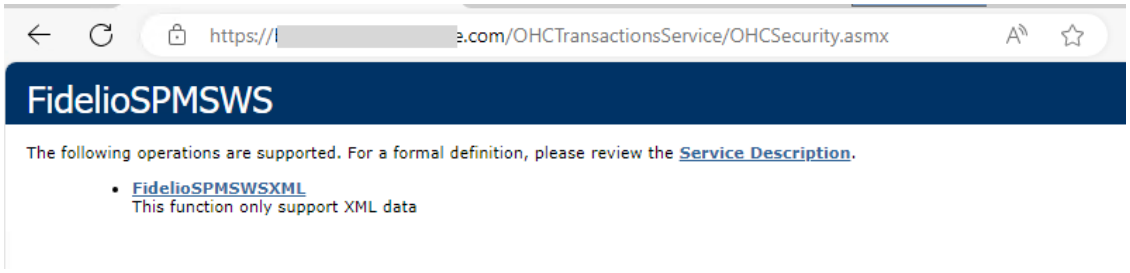
> **Note**
>
> When installing SPMS Secure Service using the **install.bat** file provided, select option **1 – Install OHCTransactionsService** to install the SPMS Secure Service required by the SPMS Secure Server.

Verifying Hosting of SPMS Secure Service

After the successful installation of the SPMS Secure Service, verify that the SPMS Secure Service is hosted correctly. If done properly, you can reach the SPMS Secure Service over the web browser using the HTTPS communication protocol.

1. From the same SPMS Secure Server machine, launch a web browser.
2. Enter this URL - `https://localhost/OHCTransactionsService/OHCSecurity.asmx`
3. If the SPMS Secure Service is hosted correctly, you will see the web page as shown below.

Figure 2-3 SPMS Secure Service Web Page Hosted on the SPMS Secure Server



> **Note**
>
> It is important to know that successful hosting of the SPMS Secure Service does not guarantee a successful SPMS Database connection, which is required for the SPMS operation. Therefore, it is important to configure the SPMS Secure Server connection to the SPMS Database.

Setting Up SPMS Secure Service Database Connection

Once you have verified that the SPMS Secure Service is hosted correctly and reachable through the web browser, configure the SPMS Secure Service so that it knows which Database TNS it should connect. This configuration resides in the web.config file.

1. In the installed Oracle Client home folder, ensure there is a correct Database TNS entry in the Oracle tnsnames.ora file. You will need the Database TNS Name entry created in the tnsnames.ora file so that SPMS can find the correct Database. To create, see below table for required parameters.

Table 2-1 User Define Parameters in Tnsnames.ora file

Tnsnames Parameters	Description
<DB_TNS_NAME>	Oracle Database TNS name. By design, SPMS applications or web services refer to the Database using the TNS name.
<DB_ADDRESS>	Address of the Oracle Database. It can be an IP address (for example, 127.0.0.1) or the machine name.
<DB_PORT>	Listener port of the Oracle Database. The port is used by the Database Server to listen for a connection.
<DB_NAME>	Oracle Database Service name. This is the name used by the Oracle Database Server to identify the Oracle Database instance.

For example:

```
<DB_TNS_NAME> = (
    DESCRIPTION = (
        ADDRESS_LIST = (
            ADDRESS = (PROTOCOL = TCP)
                      (HOST = <DB_ADDRESS>)
                      (PORT = <DB_PORT>)
        )
    )
     (CONNECT_DATA = (SERVICE_NAME = <DB_NAME>)
    )
)
```

2. The installed Oracle Client folder for SPMS is `C:/Oracle/product`. You may select to install it in a different folder.
3. You will need to set up the SPMS Secure Service Database connection. This step is needed so that the SPMS Secure Service knows which Database TNS it connects. You can do that by editing the web.config file in the `C:\inetpub\wwwroot\OHCTransactionsService` folder.
4. Under the `<appSettings>` section, set the SPMS Database TNS name.

   For example:

```
<appSettings>
     <add key="Server" value="<DB_TNS_NAME>" />
 </appSettings>
```

5. Restart the SPMS Secure Service. You can restart the SPMS Secure Service from the IIS Manager.

> **Note**
>
> After setting up the Database TNS connection for the SPMS Secure Service, the SPMS Secure Service is now able to locate the SPMS Database using the Database TNS. Note that connection to the SPMS Database is not possible yet. It needs the Database Password to be able to connect to it. To connect to the SPMS Database, the SPMS Secure Service requires the SPMS Database password, which is stored in the local DPAPI protected Secure Credential file on the SPMS Secure Server
>
> To create the local DPAPI protected Secure Credential file on the SPMS Secure Server, you are required to perform either the steps to upgrade or migrate the SPMS Database using the OHC Tools as described in Setting Up Database from SPMS 23.3 Seed Database.

Troubleshooting

The troubleshooting guide for the SPMS Secure Server is the same as for SPMS web services. See Common Errors in SPMS .NET Web Server Installation.

3

Setting Up SPMS Database Server

After setting up the SPMS Secure Server, you can prepare the SPMS Database Server for the SPMS Secure Server to connect to the SPMS Database. Currently, there are two options to prepare the SPMS Database Server.

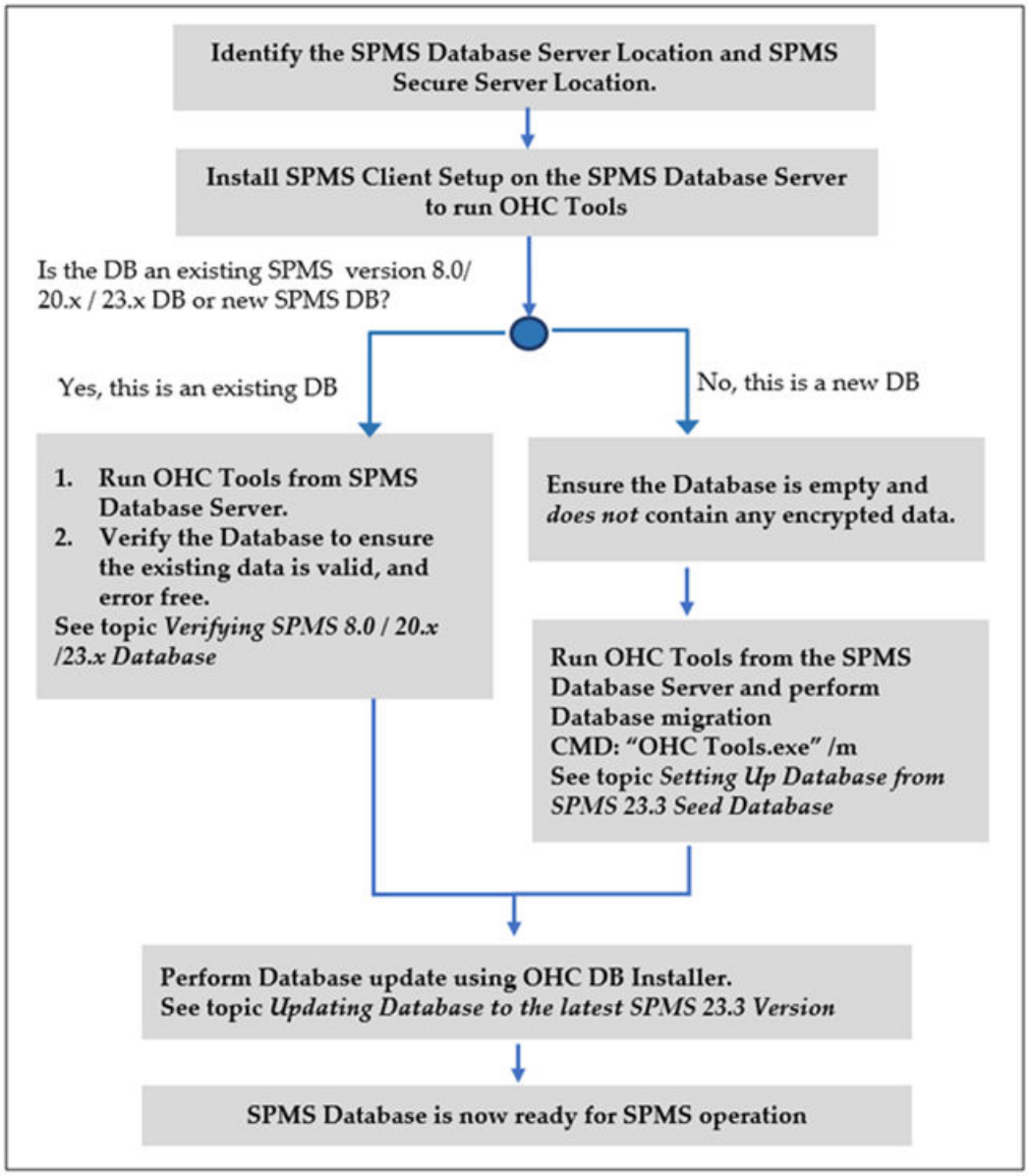
1. Upgrade from an existing SPMS 8.0 / 20.X/ 23.X Database to SPMS 23.3 Database, or
2. Set up from a seed SPMS 23.3 Database. See Definition of SPMS Seed Database in Appendix section.

Since the SPMS Database Server can be prepared from an existing SPMS 8.0 / 20.X / 23.X Database or a seed SPMS 23.3 Database, you need to understand that:

- By upgrading from an existing SPMS 8.0 / 20.X / 23.X Database, there could be existing data in the Database. Therefore, you need to validate the Database to ensure that all data is valid and error free. This method of SPMS Database setup is similar to a live ship upgrade from SPMS 8.0 / 20.X / 23.X to SPMS 23.3.
- When upgrading from a seed SPMS 23.3 Database, it should ***NOT*** contain any data in the SPMS Database. As there is no data, there will not be any SPMS Encryption Key in the SPMS Database yet. Subsequently, the Database will need to undergo a migration process to ensure that the SPMS 23.3 Database is now ready for SPMS installation. This method of SPMS Database setup is like a new ship installation with SPMS 23.3

The diagram below summarizes the process of setting up the SPMS Database Server based on the options available to you when preparing the SPMS 23.3 Database.

Figure 3-1 Database Preparation Workflow



Prerequisites

1. Oracle 19c Database Management System is installed on the target machine. It is presumed that:
   - You know where to obtain the Oracle Database Server installer.
   - You know how to install Oracle Database Server.
   - You know how to perform Oracle Database DMP import and export.
2. SPMS 23.3 Installer is downloaded and available on the target machine. See topic Where to Download in SPMS Installation File section.
3. SPMS 23.3 Package is downloaded and available in the target machine. See topic SPMS Package File.

4. Before the SPMS Database preparation, you must ensure that the DB TNS name on the client machine is the same as the DB TNS name configured on the SPMS Web Server.
5. Before you begin the SPMS Database upgrade and if you are on the below version, ensure that they are updated accordingly:
   - From SPMS v7.30x, you must update the database to v8.0.12 first before continuing.
   - From v8.0 to v8.0.11, update the database with OHC Database Installer version 8.0.12 before continuing.
   - Know the current database encryption key before you proceed to upgrade. Contact Customer Support on how to obtain an encryption key if you do not have this information.

Important

- Before you proceed, it is important to know where you intend to set up the SPMS Database Server. See topic Recommendation for the Installed SPMS Environment section for some examples of SPMS Environment configurations. The SPMS Database Server is the heart of every SPMS environment. Therefore, the first thing you need to do before installing the full SPMS environment is to identify the location of the SPMS Database Server.
- The SPMS Database Server must be reachable by all SPMS Application Clients, SPMS Secure Server, and SPMS Web Server.

SPMS Database Installation Steps

To set up the SPMS Database Server, follow the steps in the order shown below.

1. See topic Checking SPMS Database Instance.
2. See topic Verifying Connection to SPMS Database.
3. See topic Installing SPMS 23.3 Application Client on SPMS Database Server.
4. If you want to upgrade SPMS Database from version 8.0 / 20.X / 23.X to version 23.3, follow the steps below, or skip to step 5.
   - See topic Verifying SPMS 8.0 / 20.X / 23.X Database.
5. If you want to set up SPMS Database version 23.3 from a seed SPMS Database version 23.3, follow the steps below, or skip to step 6.
   - See topic Setting Up Database from SPMS 23.3 Seed Database. See also Appendix Definition of SPMS Seed Database.
6. See topic Updating Database to the latest SPMS 23.3 Version.

Checking SPMS Database Instance

The SPMS Database Server is the machine that hosts the SPMS Database Instance. Therefore, the first step to set up the SPMS Database Server is to ensure that there is already an SPMS Database Instance running on the same machine. If not, create a new Database Instance and Database Service for SPMS first. Below are the quick steps to verify that you have an SPMS Database Instance running on the SPMS Database Server machine.

This is to verify that the SPMS Database is hosted and connection can be established. To check, run the **Oracle Instance Manager** and verify that the SPMS Database Service is running.

Verifying Connection to SPMS Database

After confirming that the SPMS Database Instance is available and running, you should verify that you can connect to the SPMS Database using the SQLPlus* tool, which is installed with the Oracle Database Management System. This is important so that you can resolve any Database related issues.

All SPMS Application Clients or SPMS web services connects to the Oracle Database Instance using the TNS connection type. Therefore, ensure from the installed Oracle Client home folder that there is a correct Database TNS entry in the Oracle TNSNames.ora file.

You will need the Database TNS Name entry created in the TNSNames.ora file so that SPMS can locate the correct database when it references the Database TNS.

1. The commonly installed Oracle Client folder for SPMS is `C:/Oracle/product`. However, you may select to install it in a different folder. Now configure the Database TNS in the `TNSNames.ora` file. See Table 2-1.

```
<DB_TNS_NAME> = (
    DESCRIPTION = (
        ADDRESS_LIST = (
            ADDRESS = (PROTOCOL = TCP)
                      (HOST = <DB_ADDRESS>)
                      (PORT = <DB_PORT>)
        )
    )
     (CONNECT_DATA = (SERVICE_NAME = <DB_NAME>)
    )
)
```

2. After setting the TNS entry in the `TNSNames.ora` file, you can now verify the Database connection using Oracle SQL*Plus. The command to connect to the Database is shown below. Resolve all Database connection issues before you continue to set up the SPMS Database.

   ```
   sqlplus [DB_USER]/[DB_USER_PASSWORD]@[DB_TNS_NAME]
   ```

Installing SPMS 23.3 Application Client on SPMS Database Server

Before upgrading an existing SPMS 8.0 / 20.X / 23.X Database or prepare the SPMS 23.3 Database using a seed SPMS Database, you will need to firstly install the SPMS 23.3 Application Client on the SPMS Database Server machine. This is because you must run the SPMS OHC Tools module to perform either the Database upgrade or migration as described in the above installation steps. To install the SPMS Application Client, see chapter Setting Up SPMS Desktop Application Clients.

Verifying SPMS 8.0 / 20.X / 23.X Database

Follow the instructions below if you are preparing a database upgrade from SPMS 8.0 / 20.X / 23.X to SPMS 23.3. This step is similar to upgrading an existing ship database from SPMS 8.0 / 20.X / 23.X to SPMS 23.3

Before performing the SPMS Database upgrade, it is recommended that a Database data verification is performed first on the SPMS Database for Version 8.0 / 20.X / 23.X. This is to ensure that the data is valid and error-free before you upgrade the SPMS Database.

1. Run the **OHC Tools** program for SPMS Version 8.0 / 20.X / 23.X.
2. From the ribbon bar, select **Verify Database Encrypted Data**.
3. Select the **Service Name** and **Schema User for SPMS**, and click **Verify**.
4. Do not proceed to upgrade SPMS Database if the data verification returned failed message(s) due to invalid data. You should fix the data error and repeat the process.

   By not doing so, you acknowledge and assume the responsibility for data losses after the SPMS Database upgrade to Version 23.3.
5. Click the **Close** button when the process completes.

Setting Up Database from SPMS 23.3 Seed Database

Follow the instructions below if you are preparing a database upgrade from a seed SPMS 23.3 Database. See topic Definition of SPMS Seed Database in Appendix section. This step is same as setting up a new ship database.

1. You must ensure that SPMS Secure Service is hosted correctly and is reachable. During the SPMS Database migration process, the OHC Tools communicates with the SPMS Secure Service so that the SPMS Secure Service can create a local Secure Credential file to store the Database Password. To verify that the SPMS Secure Service is hosted and reachable, you can browse to the URL `https://[SECURE_SERVER_URL]/OHCTransactionsService/OHCSecurity.asmx` with a web browser.

   Do not proceed if the SPMS Secure Service is not reachable. Correct the web service issue before continuing. See SPMS .NET Secure Server Installation Steps
2. From the downloaded SPMS Package folder, browse to the EXE folder.
3. Copy the **OHC Tools.exe** to the SPMS installed folder `C:\Program Files (x86)\Oracle Hospitality Cruise`.
4. Run the **Windows Command Prompt** as a Windows Administrator.
5. Navigate to the folder where SPMS Application is installed. For example, `C:\Program Files (x86)\Oracle Hospitality Cruise`.
6. Run the OHC Tools Database migration using the following command. `“OHC Tools.exe” /m`.
7. This will launch OHC Tools in Migration mode comprising of two items in the Home tab - **Upgrade DPAPI Key** and **Create New Connection**.
8. Click the **Upgrade DPAPI Key** button to create a new Database entry record to both the local Secure Credential file and at the SPMS Secure Server.
9. At the Security Login prompt, select the **Database TNS** and enter the **Database Password** for authorization.
10. Key in the passphrases and click the **Update** button.
11. Upon completion, you will find that the SPMS Database password and encryption key are safely encrypted and stored by the SPMS Secure Server.

Updating Database to the latest SPMS 23.3 Version

After a successful set up of the SPMS Database for Version 23.3. The SPMS Database Installer program is a Database updater program that upgrades the SPMS Database to the latest version. Apart from performing an SPMS Database version upgrade, the Database Installer also repairs missing or invalid Database objects required by SPMS. You can find the Database Installer program as part of the SPMS Package. See SPMS Package File for download instructions.

1. From the downloaded SPMS Package folder, browse to the EXE folder.
2. Copy the **OHC Database Installer.exe** to the SPMS Installed folder `C:\Program Files (x86)\Oracle Hospitality Cruise`.

> **Note**
>
> By running the OHC Database Installer, all existing custom changes made to the database objects, index and views are repaired and restored to the default SPMS database requirement.

3. Run the Windows Explorer program and navigate to the `Oracle Hospitality Cruise` folder.
4. Double-click the **OHC Database Installer.exe** to launch the program.
5. Click the **Next** button to navigate to the next screen.
6. On the Database Connection screen, enter the **Database TNS name** and **Database Schema Password** for SPMS.
   - If the Database TNS name or Database Schema password is incorrect, you will receive an error message. Correct the information and retry.
7. To validate the Database connection, click the **Test Connection** button. A confirmation prompt appears if the connection is successful.
8. Click the **Next** button to proceed to the Options screen, and select the mode to run.
   - **Standard:** Updates the SPMS Database with the required changes.
   - **Simulation:** Checks and generate a list of changes that the system will apply. These changes will not affect the SPMS Database until you run the standard mode.
9. Click the **Next** button to proceed to the User Security Options screen.
10. On the User Security Options screen, the radio button defaults to **Backward Compatible**.
    - **Backward Compatible:** Newly added user rights for new menus will be disabled to ensure backward compatibility. Existing user rights that were added to existing menus will remain enabled. For new user rights that were reapplied to the existing menus it will be reset to the original assignment.
    - **Disable:** All Additional user rights for any new menus, as well as the existing menus will be disabled.
11. Select the right User Security option and click the **Next** button to continue. This will lead you to the Confirmation screen.
12. On the Confirm screen, click the **Next** button to start the SPMS Database Version update process. If there are SPMS applications connected to the SPMS Database, you will receive a message to reminding you to close all applications or terminate the SPMS Database connection with the application. Close all applications and click **Yes** to continue.
13. A progress window will appear, showing the status as it progresses. When the update process completes, click the **Next** button to continue.
14. When the SPMS Database Version Update completes, you will find:
    - A process log is saved in the SPMS Public Document folder `C:\Users\Public\Document\Oracle Hospitality Cruise`. Alternatively, you can click the **Copy to Clipboard** button to save the file.

- If there are new User Security Rights added to the schema, a User Security Right file will prompt upon completion of the upgrade process.

15. Click the **Finish** button to exit the SPMS Database Installer. The SPMS Database Version will be updated automatically.
16. To verify the version, log in to the SPMS Administration module and navigate to **System Setup, Database Parameters**. Information is displayed in the **System, Launcher Database Structure Version** parameter.

Troubleshooting

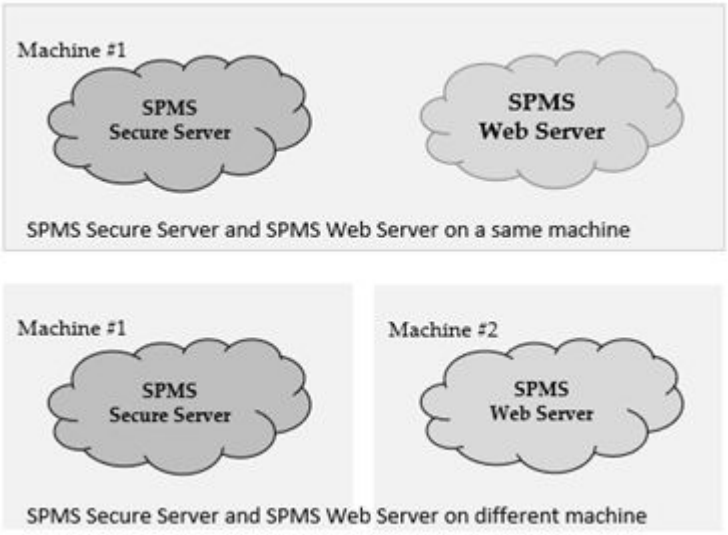
See Common Errors in SPMS Database Installation.

4

Setting Up SPMS .NET Web Server

After successfully setting up the SPMS Secure Server, you can proceed to install the SPMS Web Server. The SPMS Secure Server and SPMS Web Server are the ASP.NET web services. As they are all ASP.NET web services, they can be installed on the same IIS web server machine. As suggested in section Recommendation for the Installed SPMS Environment, you can opt to install the SPMS Secure Server in the same machine as the SPMS Web Server, or you can also install them separately in different machines.

Figure 4-1 SPMS Secure Server and Web Server Options



Prerequisites

1. Microsoft IIS is installed on the target machine.
2. Microsoft .NET Framework 2.0, 3.5 and 4.8 features are enabled on the target machine.
3. Oracle 19c Database client with ODAC is installed on the target machine. See topic Oracle Database Client and ODAC Installation.
4. SPMS Package is downloaded and available on the target machine. See topic SPMS Package File for download instructions.
5. SPMS Application Client installed. See topic Setting Up SPMS Desktop Application Clients.

SPMS .NET Web Server Installation Steps

To set up SPMS Web Server, follow the installation in the order of the steps shown below.

1. See topic Installing SPMS Web Services.

2. See topic Verifying Hosting of SPMS Web Services.
3. See topic Configuring SPMS web services Database Connection.

Installing SPMS Web Services

Follow the instructions listed below to install the SPMS web services.

1. If an earlier installation of the SPMS 7.0 / 7.30 web services exists, you are required uninstall and remove the FCTransactionsService and FCWebServices folders from the `C:\inetpub\wwwroot` folder.
2. From the downloaded SPMS Page, navigate to the Net Setup folder. See Where to Download if you have not download the package
3. Open the folder and copy the WebServer folder to the `C:\temp` folder.
4. From the `C:\temp\WebServer` folder, right-click **Install.bat** and select **Run as Administrator** to launch the Microsoft Windows command screen.
5. Select one of the option:
   - **Option 1 – Install OHCTransactionsService**, to install the SPMS Secure Service required by SPMS Secure Server. Selecting this option also installs the SPMS TransactionsService as they are packaged together.
   - **Option 2 – Install OHCWebServices**, to install the SPMS WebServices.
   - **Option 3 – Install OHCTransactionsService and OHCWebServices**, to install both the SPMS TransactionsService and WebServices.
   - **Option 4 – Install OHCOPIWebServices**, to install the SPMS OPI WebServices.
     - SPMS OPI WebServices can be installed on a load balanced environment for high availability. For guidance, refer to Setting Up Load Balancer for SPMS OPI WebServices
   - **Option 5 – Install OHCOPIDaemonService**, to install the SPMS OPI Daemon Service.
6. At the Command windows, you will be prompted to install a digital certificate for SPMS Secure Service identification.
   a. Key in ‘1’ to list the existing digital certificates installed on the machine. When the digital certificates are listed, there is a prompt message: “Please key in the subject name you want to bind”. Type the **Subject name** to bind the selected digital certificate to the SPMS Secure Service.
   b. Key in ‘2’ to create a new self-signed digital certificate and enter the domain name or IP of the SPMS Secure Server to bind the new self-signed digital certificate to the SPMS Secure Service.
7. If an older SPMS 8.0 / 20.X / 23.X Secure Service installation exists, it will prompt to override the files. Continue by selecting **All**.
8. When the installation completes, press any key to close the command prompt.

Verifying Hosting of SPMS Web Services

After the successful installation of the SPMS web services, verify that the SPMS web services are hosted correctly. If done correctly you should be able to reach the SPMS web services over the web browser using the HTTPS communication protocol.

1. Launch a web browser.
2. Type the URL shown below in the browser search bar.

a. SPMS Secure ASP.NET Web Service: The SPMS Secure Service is the web service that manages the database user credentials. Clients that require a database connection will interact with the Secure Server to obtain the database user credential. It is typically deployed at `https://[URL]/OHCTransactionsService/OHCSecurity.asmx`

b. SPMS OHCTransactionsService ASP.NET Web Service: The SPMS OHCTransactionsService is the web service that serves internal client requests. It is typically deployed at `https://[URL]/OHCTransactionsService/OHCTransactionsService.asmx`

c. SPMS OHCWebServices ASP.NET Web Service: The SPMS OHCWebServices is the web service that serves external client requests. It is typically deployed at `https://[URL]/OHCWebServices/OHCWebServices.asmx`

3. If the SPMS web services are hosted successfully, a web page will appear as shown in SPMS Secure Service Web Page Hosted on the SPMS Secure Server.

> **Note**
>
> It is important to know that successful hosting of the SPMS web services does not guarantee a successful SPMS Database connection, which is required for SPMS operation. Therefore, it is important to configure the SPMS web services connection to the SPMS Database.

Configuring SPMS web services Database Connection

Once you have verified that the SPMS web services are hosted correctly and reachable through the web browser, you can then proceed to configure the SPMS web services so that it knows which Database TNS it connects to. Like most web services, this configuration resides in the usual web.config file.

1. From the installed Oracle Client home folder, ensure there is a correct Database TNS entry in the `Oracle TNSNames.ora` file for SPMS to locate the correct Database when it references to the Database TNS.
2. If the Database TNS entry is not in the `TNSNames.ora` file, you can create it using the below example. See also User Define Parameters in Tnsnames.ora file

```
<DB_TNS_NAME> = (
      DESCRIPTION = (
          ADDRESS_LIST = (
              ADDRESS = (PROTOCOL = TCP)
                        (HOST = <DB_ADDRESS>)
                        (PORT = <DB_PORT>)
          )
      )
       (CONNECT_DATA = (SERVICE_NAME = <DB_NAME>)
      )
  )
```

3. The commonly installed Oracle Client folder for SPMS is `C:/Oracle/product`. However, you can select to install it to a different folder.

4. After that, continue to set up the SPMS Web Services Database connection. This step is required for the SPMS Web Services to know which Database TNS it should connect to. You can do that by editing the web.config file.

   The web.config file for SPMS OHCTransactionsService resides in `C:\inetpub\wwwroot\OHCTransactionsService` and the web.config file for SPMS OHCWebServices resides in `C:\inetpub\wwwroot\OHCWebServices` folder.

5. Under the `<appSettings>` section of the web.config file, set the SPMS Database TNS name.

   For example:

```
<appSettings>
    <add key="Server" value="<DB_TNS_NAME>" />
</appSettings>
```

> **Note**
>
> After setting up the Database TNS connection for SPMS web services, the SPMS web services are now able to find the SPMS Database using the Database TNS. Note that the connection to the SPMS Database is not possible yet. It needs the Database Password to be able to connect to it.
>
> To connect to the SPMS Database, the SPMS web services would require the SPMS Database password, which is stored in the local DPAPI protected Secure Credential file on the SPMS Web Server.
>
> To create the local DPAPI protected Secure Credential file on the SPMS Web Server, you must connect to the SPMS Secure Server which can be configured from the same web.config file.

6. Under the `<appSettings>` section of the web.config file, set the SPMS Secure Server IP address or the machine name.

Table 4-1 User Definable Value in Web.Config File

Web.Config File Value	Description
<SECURE_SERVER_NAME>	A User defined SPMS Secure Server IP address or the machine name if it is resolvable by the DNS server.

   For example:

```
<appSettings>
    <add key=" SecureLogin" value="<SECURE_SERVER_NAME>" />
</appSettings>
```

7. Restart the SPMS web services. You can restart the SPMS Secure Service from the IIS Manager.

Configuring SPMS OPI Web Services Database Access

OPI Web Services/APIs uses the Oracle.ManagedDataAccess.Client data provider to connect to the database. Therefore, you need to ensure that the “ODP.NET, Managed Driver” section is configured correctly on the local machine.

On an older Oracle 12c Database Client installation, the section below will automatically populate at "C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config". Thus, no further action is needed. However, for the newer Oracle 19c Database Client, you must *uncomment* the following configuration in the "web.config" file of the OPI Web Service. Additionally, ensure that the Version is set correctly to match the DLL version installed on the local machine.

```
<system.data>
    <DbProviderFactories>
      <add name="ODP.NET, Managed Driver"
invariant="Oracle.ManagedDataAccess.Client" description="Oracle Data Provider
for .NET, Managed Driver"
type="Oracle.ManagedDataAccess.Client.OracleClientFactory,
Oracle.ManagedDataAccess, Version=<DLL_VERSION>, Culture=neutral,
PublicKeyToken=89b483f429c47342" />
      <add name="ODP.NET, Unmanaged Driver"
invariant="Oracle.DataAccess.Client" description="Oracle Data Provider
for .NET, Unmanaged Driver"
type="Oracle.DataAccess.Client.OracleClientFactory, Oracle.DataAccess,
Version=<dll version>, Culture=neutral, PublicKeyToken=89b483f429c47342" />
    </DbProviderFactories>
  </system.data>
```

Configuring SPMS OPI WebServices Database Connection for OPI Handling

Edit the web.config file in `C:\inetpub\OHCOPIWebServices` and to define the SPMS database server name <SOURCE>, password<PASSWORD> and User ID <DBUSER> under <connectionStrings>.

```
<connectionStrings>
<add name="OHCEntities" connectionString="metadata=<a target="_blank"
href="res://*/OHCModel.csdl|res://*/OHCModel.ssdl|res://*/
OHCModel.msl;provider=Oracle.ManagedDataAccess.Client;provider">res://*/
OHCModel.csdl|res://*/OHCModel.ssdl|res://*/
OHCModel.msl;provider=Oracle.ManagedDataAccess.Client;provider</a> connection
string=&quot;DATA SOURCE=[SOURCE];PASSWORD=[PASSWORD];PERSIST SECURITY
INFO=True;USER ID=<USER ID>&quot;" providerName="System.Data.EntityClient" />
</connectionStrings>
```

If Oracle Wallet is applied:

```
<connectionStrings>
<add name="OHCEntities" connectionString="metadata=<a target="_blank"
href="res://*/OHCModel.csdl|res://*/OHCModel.ssdl|res://*/
OHCModel.msl;provider=Oracle.ManagedDataAccess.Client;provider">res://*/
OHCModel.csdl|res://*/OHCModel.ssdl|res://*/
OHCModel.msl;provider=Oracle.ManagedDataAccess.Client;provider</a> connection
string=&quot;DATA SOURCE=<IP Address>:<Port No>/<Service
Name>;PASSWORD=[PASSWORD];PERSIST SECURITY INFO=True;USER ID=<User ID>&quot;"
providerName="System.Data.
```

Configuring SPMS OPI Web Services Token Expiry for OPI Handling

By default, the OPI Web Service token expires after 1440 minutes (1 day); the refresh token expires in 2880 minutes (2 days). The refresh token expiry value must be greater than the token.

To define the token expiry, edit the web.config file in `C:\inetpub\OHCOPIWebServices` and insert below keys and value:

```
<add key="TokenExpiry" value="1440"/>
```

```
<add key="RefreshTokenExpiry" value="2880"/>
```

The OPI Manager and Universal Interface which runs on the server utilizes the refresh token functionality to ensure the connection to the OPI web service remains active.

The system triggers the token refresh 2 minutes before it expires.

To ensure the OPI Web Service token is always valid at other SPMS client applications, the value of TokenExpiry must be greater than the parameter “Idle Minutes.”

Troubleshooting

See Common Errors in SPMS .NET Web Server Installation.

5

Setting Up SPMS Desktop Application Clients

The SPMS Application Clients can be installed on any machines that have the full Oracle Client installed, including the Oracle Data Access Components (ODAC) component.

Prerequisites

1. Ensure you uninstall all the components older than SPMS 23.3. However, if you choose not to uninstall, you may follow the steps depicted in section Alternate option to upgrade existing SPMS Desktop Application Clients version 23.1.0 or later.
2. Ensure that the Microsoft .NET Framework 2 and 3.5 and 4.8 are enabled in Window Features before installing Oracle Full Client and **CruisePropertyManagementDesktopApps_23.3.exe** file.
3. Oracle 19c Database client with ODAC is installed on the target machine. See topic Oracle Database Client and ODAC Installation.
4. SAP Crystal Report runtime engine for .NET Framework (32-bits) version 13.0.33 is installed on the target machine. See How to Install/ Upgrade Crystal Reports runtime engine for .NET Framework (32-bit) for further information.
5. SPMS 23.3 Installer is downloaded and available in the target machine. See topic SPMS Installation File for download instructions.
6. SPMS 23.3 Package is downloaded and available in the target machine. See topic SPMS Package File for download instructions.
7. Ensure that the Windows Regional and Language Settings on the target machine is configured to US/UK and the language setting is set to English. This important to ensure that you get the expected SPMS functionality.

SPMS Desktop Application Clients Installation Steps

The SPMS Desktop Application Clients Installer is now available in two formats: EXE or MSI format. MSI format is a Windows Installer format that uses Microsoft's Windows Installer service to configure or update installer packages. MSI format is the preferred format by Windows users to distribute in enterprise environments.

Install Desktop Apps (EXE file path) through Windows Batch File

Installing via the batch file will be the preferred method to install SPMS Application Client. Alternatively, SPMS Application Client can be installed manually from the UI. To install, just run the (InstallDesktopClient.bat) batch file and leave it unattended until installation completes.

> **Note**
>
> The InstallDesktopClient.bat does two things: Uninstalling older version of SPMS Application Client, and installing new SPMS Application Client.
>
> The command to install SPMS Application Client silently. is
>
> ```
> CruisePropertyManagementDesktopApps_23.3.exe /s /v"/qn /log
> "SPMS23.3.log"
> ```

Follow the instructions below to install the SPMS Application Client:

1. Download both the SPMS Installer and Package. See topic Where to Download to prepare the SPMS 23.3 Application Client Installation Package.
2. To prepare the SPMS Application Client Installation Package, copy the SPMSClientInstall folder from the SPMS Package to the `C:\Temp` folder.
3. Copy the SPMS Installer: **CruisePropertyManagementDesktopApps_23.3.exe** to the `C:\Temp\SPMSClientInstall` folder. The folder is now ready for SPMS Application Client installation.
4. After this, you may copy the SPMSClientInstall folder to other target machines that require SPMS Application Client installation.

> **Note**
>
> You will only need to prepare the SPMS Application Client Installation Package once. Once you have the package ready, you can remotely copy the package to any target machine and run the one-step SPMS Application Client installation remotely.

5. You can now start the unattended one-step installation of the SPMS Application Client by navigating to the `C:\Temp\SPMSClientInstall\` folder.
6. Run the **InstallDesktopClient.bat** with the Windows Administrative privilege by right-clicking the file and selecting **Run as Administrator**.

> **Note**
>
> You may refer to the batch file to get the commands used to uninstall or install SPMS Application Client. Two options are provided for uninstallation: **wmic uninstall** method, or the Powershell **Uninstall-Package** cmdlet.
>
> Powershell method is faster and is the default method to uninstall. By commenting out the variable FAST_INSTALL, the batch file will switch to use wmic uninstall method.
>
> *You need to uncomment the 23.1 / 23.2 Uninstall portion from the batch file if you want to run a Maintenance for 23.3 as the product name at Control Panel for SPMS 23.1x, SPMS 23.2.x and SPMS 23.3 is same.*

7. Once the installation starts, leave it running unattended until it completes.

8. After installing the SPMS Application Client, a Windows Scheduled Task is created to handle the SPMS DLLs registration automatically.
9. For customers who wish to have both SPMS 7.0 / 7.30 and 23.3 Application Clients exist on the same machine, you can run the `CreateSchTasksToRegSpmsOldNew.bat` file to create another Windows Scheduled Task to handle the SPMS 7.0 / 7.30 DLLs registration automatically. The batch file shown below resides in `RegisterSpms` folder of the SPMS installed directory.

> **Note**
>
> The Windows Scheduled Task, **Cruise Property Management 7.X Desktop Apps Registration** will auto-register SPMS components for SPMS Version 7.0 / 7.30 and below.
>
> The Windows Scheduled Task, **Cruise Property Management Desktop Apps Registration** will auto-register SPMS components for SPMS Version 8.0 / 20.X / 23.X and above.
>
> If you intend to run both the SPMS Application Client Version 7.0 / 7.30, and Version 8.0 / 20.X / 23.X or later on the same machine, you **must** disable the SPMS Version 7.0 / 7.30 FC Updater from running as it will interfere with the auto-registration of the SPMS DLLs in Windows Scheduled Tasks.

10. To disable SPMS Version 7.0 / 7.30, navigate to the SPMS Installed folder for Version 7.0 / 7.30 and rename the **“FC Updater.exe”** file to **“FC Updater.exe.bak”**

Install Desktop App Installer in MSI format using Windows MSIEXEC command

For Windows user who prefers to install SPMS Desktop Application Client using MSI format, the standard Windows installer package command msiexec is recommended. Follow the instructions below to install the SPMS Application Client.

1. Download both the SPMS Installer and Package. See topic Where to Download to prepare the SPMS 23.3 Application Client Installation Package.
2. Copy the SPMS Installer — **CruisePropertyManagementDesktopApps_23.3.msi** file to the `C:\Temp` folder.
3. Call the MSIEXEC command to install. For command details, see: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

Alternate option to upgrade existing SPMS Desktop Application Clients version 23.2.0 or later

For existing SPMS 23.1 / 23.2 users, uninstallation of the SPMS 23.1 / 23.2 Desktop Application Client is not necessary as it is compatible with SPMS 23.3 Desktop Application Client. You may opt to apply the SPMS 23.3 Desktop Application Client directly without uninstalling earlier version.

However, due to a newer version of `BouncyCastle.Cryptography.dll` being used in SPMS 23.2, user upgrading from **version SPMS23.1 must** upload the DLL file to the SPMS Database so that OHC Updater can distribute it automatically to other clients.

> **Important**
>
> Before proceeding, ensure that:
>
> - The SPMS Database is updated to version 23.3 through the running of OHC Database Installer before proceeding.
> - The SPMS Secure Server and SPMS Web Server are updated to version 23.3.

Follow the instructions below to apply the SPMS 23.3 Application Client:

1. Extract the earlier downloaded SPMS 23.3 Package to `C:\Temp\SPMS.23.3\`. See topic Where to Download if you do not already have the package.
2. Run **OHC Launch Panel** version 23.3 by navigating to `C:\Program Files (x86)\Oracle Hospitality Cruise` folder, launch the **Launch Panel** and log in using Bypass Updater mode, that is by holding down the **ALT Key + clicking** the female user icon.
3. In the Launch Panel program, press the **F12** key to upload
   a. BouncyCastle.Cryptography.dll from the `C:\Temp\SPMS.23.3\Net Setup\WebServer\OHCWebServices\bin` folder to SPMS Database for automatic distribution to all other clients. Upload the `BouncyCastle.Cryptography.dll` as a **System Files type**.

   > **Note**
   >
   > If you are upgrading from version SPMS 23.1, you **must not** skip this step.

   b. upload all other required **SPMS EXEs and DLLs** to SPMS Database for automatic distribution to all other clients from `C:\Temp\SPMS.23.3\DLLs` and `C:\Temp\SPMS.23.3\EXE`.
4. SPMS 23.3 Desktop Application Client is now ready to run.

Switching between SPMS Application Clients Versions

Before SPMS Version 8.0.14, it was only possible to run one version of SPMS Application Client on the same machine. To switch to another SPMS Application Client version, users **must** perform a manual registration of the SPMS DLLs, which require Windows Administrative privilege. This is not ideal because to have more than one version of SPMS Application Client on one machine, users must be granted Windows Administrative privilege.

From SPMS Version 8.0.14 onwards, it is now possible to have both SPMS Application Client Version 7.0 / 7.30 and Version 8.0 / 20.X / 23.X on the same machine, without needing to grant Windows Administrative privilege to the users, as the DLLs registration is now automated by the Windows Scheduled Tasks. Therefore, the users no longer require Windows Administrative privileges to switch between SPMS Versions.

When switching from SPMS Application Client Version 7.0 / 7.30 to SPMS Application Client Version 8.0 / 20.X / 23.X, the Windows Scheduled Task triggers the **Cruise Property Management Desktop Apps Registration** batch file, thus, registering the required SPMS DLL, automatically using the Windows SYSTEM privilege.

Similarly, when switching from SPMS Application Client Version 8.0 / 20.X / 23.X to Version 7.0 / 7.30, the Windows Scheduled Task triggers the **Cruise Property Management 7.X**

Desktop Apps Registration batch file, thereby, automatically registering the required SPMS DLLs using the Windows SYSTEM privilege.

Switching to SPMS Application Client version 7.0 / 7.30

1. Run the FC Launch Panel of SPMS Version 7.0 / 7.30.
2. Once launched, a prompt appears, notifying you that the SPMS DLLs registration process will take place. You are to *wait* for the next message prompt before proceeding to the next step.
3. Once the DLL registration completes, a new message prompt appears, notifying you the registration process has complete. Click **OK** to close.
4. Follow the instructions in the message prompt and relaunch the FC Launch Panel for SPMS Version 7.0 / 7.30.

> **Note**
>
> If you did not get the message prompts, navigate to the folder `C:\tempDLL` and check whether the folder `RegisteredSPMSv7_3` exists.

5. If the folder `RegisteredSPMSv7_3` exists, this means that the SPMS DLLs are registered successfully, and you can relaunch the **FC Launch Panel for Version 7.0 / 7.30**.

Switching to SPMS Application Client version 8.0 / 20.X / 23.X

1. Launch the version of **OHC Launch Panel** you wish to work on from the `Oracle Hospitality Cruise` folder.
2. Once the program opens, you will receive a notification prompt that registering the SPMS DLLs will take place.
3. Click **OK** and wait for the next message prompt before continuing. You will receive a confirmation prompt once the registration process completes.
4. Click **OK** to close the message and proceed to relaunch the SPMS application.
5. Follow the instruction in the message prompt and relaunch the OHC Launch Panel for SPMS Version 8.0 / 20.X / 23.X.

> **Note**
>
> If you did not get the message prompts, navigate to the folder `C:\tempDLL` and check whether the folder `RegisteredSPMSv8_0` exists.

6. If the folder `RegisteredSPMSvNew` exists, this means the SPMS DLLs are registered successfully and you can relaunch the **OHC Launch Panel for Version 8.0 / 20.X / 23.X**.

Loading DLLs from SPMS Allowlisted Path

This feature is designed to prevent an unscrupulous party from performing a malicious attack on the SPMS application through DLLs replacement. By default, SPMS will allow DLLs from the following repository:

1. `C:\Windows,`

2. `C:\Program Files`,
3. `C:\Program Files (x86)`,
4. `C:\Oracle`

Therefore, it is of utmost importance that you ensure the four folders above has Administrator level write access.

Should you intend to have an allowlist path other than the listed four, you should create an allowlist file (path.env) in the SPMS Installed folder – `C:\Program Files (x86)\Oracle Hospitality Cruise`.

The format of the allowlist entry path is shown below. Each path is delimited with a semicolon character.

```
<AllowlistPath1>;<AllowlistPath2>;<AllowlistPathN>
```

You can refer to the `SPMSClientInstall` folder in the SPMS Package for a sample path.env file.

Connecting to different SPMS Database using different TNS

It is now possible for SPMS Application Client to easily connect to different SPMS Databases using different Database TNS Names by creating a new Database entry in the local Secure Credential file using a different Database TNS Name from the actual Database TNS Name used in the SPMS Database Server. With this, the SPMS Application Client can connect to the SPMS Database using a TNS Name different from the actual Database TNS Name used in the SPMS Database Server.

Adding new Database TNS to the Local Secure Credential

> **Note**
>
> For each local Windows user that runs SPMS application, you need to perform the below steps to ensure the new entry for the Windows user is added to the local Secure Credential file.

1. Using the Windows Administrative privileges, run the command `"OHC Tools.exe" /m`.
2. On the OHC Tools Main screen, click the **Create New Connection** button to create a new Database entry in the local Secure Credential file using a different Database TNS Name
3. At the Create New Connection window, enter the following:
   - **New Connection:** The new DB TNS Name.
   - **Current Connection:** Existing DB TNS Name.
   - **Database Password:** Current DB Password.
4. After clicking the **Login** button, the SPMS User Authorization form appears.
5. You must authorize using the SPMS Login credential to create a new Database entry to the local Secure Credential file using a different Database TNS Name.
6. After the process completes, you can now connect to the same SPMS Database using the new Database TNS Name.

Uploading SPMS Applications or Libraries to Database

For the OHC Updater to automatically download the latest binaries or files on all SPMS Application Client machines, follow the instructions below to upload binaries or files to the SPMS Database.

1. Navigate to `C:\Program Files (x86)\Oracle Hospitality Cruise` folder, launch the **Launch Panel** and log in using a Bypass Updater, by holding down the **ALT Key + clicking** the female user icon.
2. In the Launch Panel program, manually add the following SPMS applications and DLLs to the respective group by pressing **F12** and selecting the group from the drop-down list:
   a. For **Utilities** group:
      i. OHC UpdaterWatchdog.exe
   b. For **System Files** group:
      i. OHCSPMSMobile.dll
      ii. OHCSPMSUI.dll
      iii. OHCWebSockets.dll
   c. **For REGASM Files group:**
      i. CRUFLFC.dll
      ii. OHCSPMSData.dll
      iii. OHCSPMSBusiness.dll
      iv. OHCSPMSUtils.dll
   d. **For Special Applications File group:**
      i. OHC Updater.ini

   > **Note**
   >
   > You need to upload the OHC Updater.ini to the Special Applications Files group if the file is distributed in the package for a patch or hot fix to be applied.
   >
   > All libraries or EXE files added using **F12** will appear under the "Special Applications" group by default. This is the standard application behavior.

3. Additionally, on the **Launch Panel, Utilities tab**, update the **Launch Panel, Updater**, and **UpdaterAgent** to the latest program file from the downloaded patch set by right-clicking the program and selecting **Properties**. Click **Update file** and then click **OK** to save.

Downloading SPMS Applications or Libraries from Database

Follow the instructions listed below to download the latest binaries or files from the SPMS Database to the SPMS Application Client machine.

1. On the target SPMS Application Client machine, log in to **Launch Panel without Bypass Updater** to update all the programs.

2. A program **UpdaterWatchdog** is added to monitor and ensure the **Updater** remains active in the Task Manager, enabling the latest program to be downloaded from SPMS Database. If the Standard User cannot connect to the Updater, reinstall the SPMS Application Client

   See topic: Install Desktop Apps (EXE format) through Windows Batch File in SPMS Desktop Application Clients Installation Steps

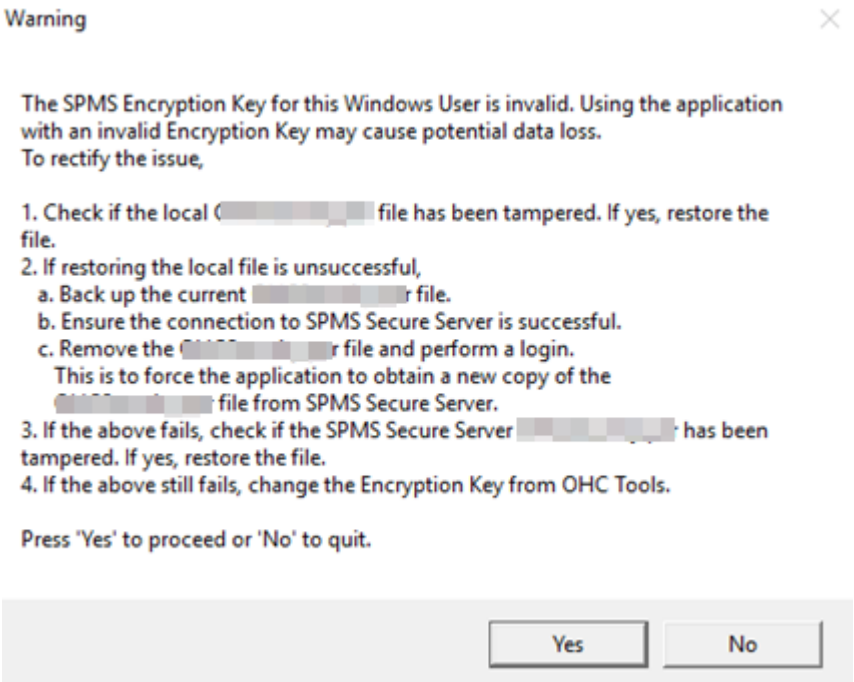
Converting Credit Card Payment from Non-OPI to OPI Tokenization

1. Set up the OPI in SPMS. See topic: OPI Handling User Guide in the Oracle Help Center.
2. Convert the existing credit card records to OPI Token at the **Get Token** tab.
   a. Select profile type and reservation to process.
   b. Click the **Start** button to start the process.
   c. Purge all OPI log files from `C:\Users\Public\Documents\Oracle Hospitality Cruise` folder.

Working with Invalid SPMS Encryption Key

SPMS Encryption Key is securely stored in SPMS Secure Server and SPMS Database. The system will prompt a warning if the SPMS Encryption Key is found to have been tampered with and the key becomes invalid. The steps to resolve the invalid key is shown in the Warning prompt.

Figure 5-1 Invalid SPMS Encryption Key Warning



Uninstalling SPMS Application Client

The following section describes the steps to remove the SPMS programs. If you want to completely remove SPMS from your servers, you must manually delete the SPMS database components from the database after uninstalling the application.

1. Open the **Control Panel** and select **Programs, Programs and Features**.
2. Select **Oracle Hospitality Cruise Property Management Desktop Apps** from the program listed.
3. Click **Uninstall** on the menu bar.
4. Follow the instructions on the screen.

Troubleshooting

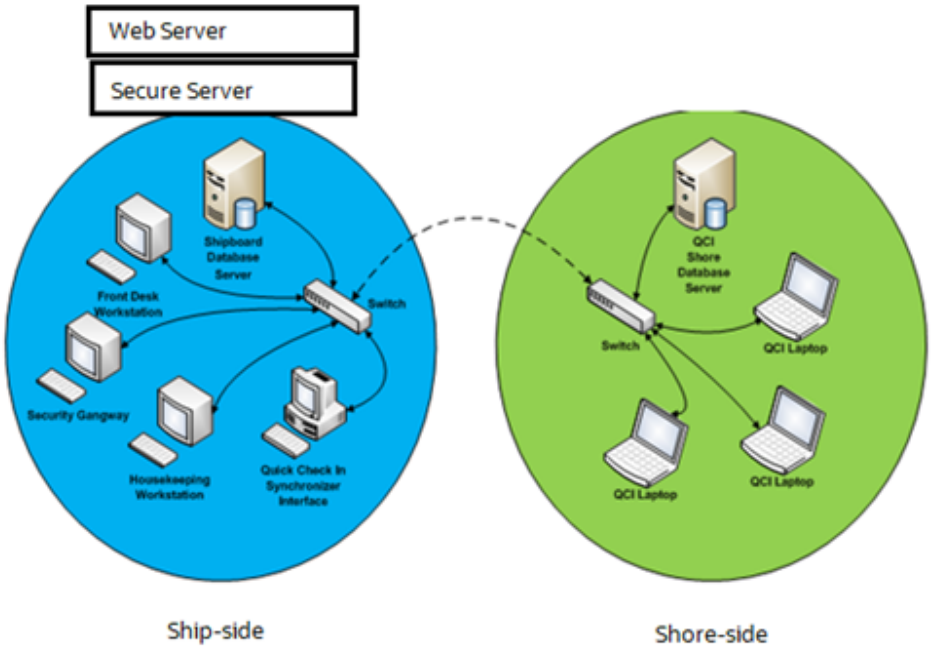
See Common Errors in SPMS Desktop Application Client Installation.

6

Setting Up SPMS QCI Offline Operation

In SPMS, there is a feature that allows the shore side client machines to continue operating in real-time, even in an off-line mode, where there is no connection to the ship side SPMS Database Server.

Figure 6-1 SPMS QCI Offline Operation



To support this, you need an additional Database Server that must be placed on the shore side, as depicted in the diagram above. On the shore-side, only the Database Server is required. SPMS Web Server and Secure Server do not to be placed on the shore side.

Prerequisites

- The version of Oracle Database Edition of the QCI Shore database and Ship database must be identical. For example; if the ship is running on Oracle 19c then the shore QCI database must also run on Oracle 19c.
- Both the Ship database and the QCI Shore database password must be identical. If a different password is used, the connection will show *Disconnected*.

Setting Up QCI Shore Database and QCI Secure Server

To set up the QCI Shore database, See topic Setting Up SPMS Database Server. The steps are similar to the setup of the ship side SPMS Database. When setting up the QCI Shore

Database, you may use the TNS name like ShoreDB to point to the QCI Shore Database The server must be pre-installed with SPMS Web Service. In web.config, define the Connection Name of the Shore Database (ShoreDB) at Server and define Shore WebService IP at SecureLogin. This is to make sure the server acts as Secure Server when hosted on shore side.

The server must be:

- Pre-installed with SPMS for OHC Tools and OHC Advanced Quick Check In. The securelogin.txt must point to QCI Shore Database Server's web server.
- Run the Windows Command Prompt as a Windows Administrator. Navigate to the Installed SPMS Application folder. For example, `C:\Program Files (x86)\Oracle Hospitality Cruise`. Run the **OHC Tools** using the following command: `"OHC Tools.exe" /m`.
- Click the **Upgrade DPAPI Key** button. At the Security Login prompt, choose the **Shore Database TNS** and enter the **Database Password** for authorization.
- Key in the passphrase and click the **Update** button. The passphrase **MUST** be same as Ship database.
- Upon completion, the encryption password and encryption key are stored in QCI Shore Database Server's Web Server.

> **Note**
>
> When setting up to the database on the shoreside, use the same TNS name and DB Password as the ship application. For example, if the TNS name "SPMSv8DB" is used at the shipside to connect to the Ship database, then you must use the same TNS name "SPMSv8DB" at the shoreside for the QCI Shore database.
>
> This allows any QCI laptop to obtain the database password from the Secure Server at the shipside and write to the database when there is a network connection.

Setting Up QCI Shore SPMS Application Client

As depicted in Figure 6-1, the QCI laptops must connect to the QCI Shore Database to operate. To set up the QCI Shore SPMS Application Client, see topic SPMS Desktop Application Clients Installation Steps.

When setting up, the TNS name pointing to the QCI Shore Database must be the TNS name used on the QCI Shore Database. On the SecureLogin.txt file, the IP of the Secure Server on shore side must be added to allow the QCI laptop to request the database password from the Secure Server of the shore side if it **does not have** a copy of the database password stored on the local DPAPI protected Secure Credential file.

> **Note**
>
> SPMS Application Client on the QCI laptops is able to connect to multiple Databases at shoreside. You can set up the TNS for each of the Databases.
>
> If there are other ship using the same SID of shore database, for example, Ship A and Ship B connect using the same TNS name that used to reference the QCI Shore database and before you perform a new Start Offline Mode on each ship, remove the Secure Credential file in QCI Shore Server if that exist and restart the IIS. Ensure the Secure Credential file at all check in terminals are removed too.

Setting Up Shipside QCI Synchronization Interface

As depicted in Figure 7–1, a ship side machine is dedicated to run the QCI Synchronization Interface. To set up the QCI Synchronization Interface, see topic SPMS Desktop Application Clients Installation Steps. The SPMS QCI Synchronization Interface requires connection to both the Ship database and QCI Shore Database. Therefore, the TNS Name used for the Ship database and QCI Shore Database must be different in this local machine.

7

Installing SPMS REST API/Web Application Server

Prerequisites

- The time zone of both the Web Application server and API server must be the same. If multiple Web Application servers and/or multiple API servers are setup, their time zones must be the same. It is recommended that you use the database server time zone.
- The SPMS Database must be on version 23.3. If you are running on version lower than the stated, upgrade the SPMS database version before continuing.
- The Web application server and API server do not require IIS.
- Java JDK version 17.0.4 and above is required.
- A tool for generating certificates. As an example, this document uses a custom tool JSON Web Key (JWK) for our internal team to generate JWK. Other tools are available. We recommend that you select a tool that suits your security requirements. Whichever tool you use, ensure that it is virus scanned and virus-free, up to date, and patch with the latest security fixes. Otherwise, you could compromise your environment.
- The API and Web application access uses a Secure Socket Layer and Transport Layer Security (SSL/TSL) cryptographic protocol. You must set up a keystore (.jks format) that contains the private key and certificate.
- The keystore must have the default option value as “`-keyalg RSA -keysize 2048`”.
- A public (verify-jwk.json) and private key (sign-jwk.json) for setting up secure OAUTH. As an example, this document explains how to generate a public and private key.

Preparing the Java Environment

Before you install the SPMS API/Apps server,

1. Ensure the JDK is installed.
2. Ensure that you have a tool for manipulating certificates installed.

Setting JAVA_HOME or JRE_HOME environment variable

1. Located our Java installation directory.
2. Press **Windows logo key + R** key to open the **Run** dialog.
3. Type **sysdm.cpl** in the input field and click **OK**
4. At the System Properties dialog, go to **Advanced tab**.
5. Click the **Environment Variables** button.
6. Under System Variables section, look for JAVA_HOME or JRE_HOME variable.
7. If it exists, click the **Edit** button to open the **Edit System Variable** window.
8. Otherwise click **New** button to open the New System Variable dialog.
9. On the New/Edit System variable dialog, **Variable name** field, insert one of the following:

- **JAVA_HOME** if you have the JDK (Java Development Kit) installed.
- **JRE_HOME** if you have the JRE (Java Runtime Environment) installed.
- For the **Variable value** click the **Browse Directory** and select the JDK/JRE installation folder, for example `"C:\Program Files\Java\[java version]"`

10. Click **OK** to apply the changes.

Adding Java to System Path

1. Click the **Environment Variables** button, then select **Edit** to edit the system environment variable.
2. Under System Variables, located the 'Path' then click **Edit**.
3. At the Edit environment variable window, select **New**.
4. Insert `%JAVA_HOME%\bin` or `%JRE_HOME%\bin` to the path.
5. If multiple Java directory entries is present, move this directory to the top of the list using the **Move Up/Move Down** button.
6. Click **OK** to apply the change.

Check Java Path

To list the different Java versions and installed path, launch the Windows Command and at the prompt, enter "where java". The first in the list will be used by the API. Move the required Java version above the other directories. See Adding Java to System Path section on how to move the directory.

Installation Process

Installation is a three-step process, where:

- **Step 1:** Create a Java keystore containing certificates purchased from a reputable Certificate Authority
- **Step 2:** Generate security keys for OAuth
- **Step 3:** Install the software

Step 1: Create the Java Keystore for SPMS API/Apps Server

Background

Java Keystore is required to store private keys and certificates used by the SPMS Version API/ Apps server. A Java's Keytool is used to create a Java Keystore. Java's Keytool is distributed as part of the Java JDK. Java Keystore files can be generated on any machine. They need not be on the same server where the SSL/TLS certificate will be installed.

Important: In this section, we use OpenSSL to demonstrate the process. You should select a certification manipulation tool that meets your organization's security policy.

Recommendations

It is recommended that you generate a new Keystore following the process outlined in this section. Installing a new certificate to an existing Keystore often ends in installation errors or the SSL/TLS certificate not working properly. Before you begin this process, backup and remove any old Keystores.

The act of generating a self-signed Digital Certificate to identify the SPMS API/Apps Server is not recommended for the production environment. It increases the risk of an unscrupulous party impersonating the SPMS API/Apps to steal sensitive information. However, for limited, non- production testing of SPMS API/Apps, you could use a self-signed certificate despite the increased security risk. However, do so at your own risk: this is not recommended.

Generate a new Java Keystore using Java Keytool

> **Note**
>
> Single domain certificate is more secure than multi-domain and wildcard certificate.
>
> When a private key of a multi-domain or wildcard certificate is compromised, this will put all domains, sub-domains and sessions covered by the certificate in risk. Proper key management and security measures are essential to mitigate this risk.

1. Navigate to the directory where you plan to manage your Keystore and SSL/TLS certificates.
2. Run the following command:

   ```
   keytool -genkey -alias <ALIAS> -keyalg RSA -keysize 2048 -keystore
   <SITE_NAME>.jks –ext SAN=dns:<SITE_NAME>
   ```

3. In the command above, `<SITE_NAME>` represents the domain name to be secured with the SSL/TLS certificate. The asterisk (*) character should not be included in the `<SITE_NAME>` as it is not a valid character in the Keytool command. The command generates a Keystore containing a public and private key pair, along with a self-signed certificate for the server. `<ALIAS>` is the name for the newly created entry in the Keystore.
4. You will be prompted to create a password for the new Keystore.
5. Enter the SSL/TLS certificate information for the self-signed certificate.
   a. When prompted for the first and last name, enter the Fully Qualified Domain Name (FQDN) for the site you wish to secure with the SSL/TLS certificate. For example, `www.yourdomain.com` or `mail.yourdomain.com`.
   b. Enter the Common Name (CN), for example, The FQDN.
   c. Enter the Organizational Unit (OU), for example, Cruise Operation
   d. Enter the Organization (O), for example, Cruise Company
   e. Enter the Locality (L). For example Redwood City
   f. Enter the State or Province Name (S), for example, California
   g. Enter the Country Name (C), for example. US
   h. You will be prompted to verify all the information entered. Type ‘y’ or ‘yes’ to confirm.
   i. Enter the Keystore password when prompt. The new Keystore file `<SITE_NAME>.jks` is now available in the current working directory.

Generate a Certificate Signing Request (CSR) using Java Keytool

1. Navigate to the directory where the Keystore was generated earlier.
2. Run the following command:

```
keytool -certreq -alias <ALIAS> -file csr.txt -keystore <SITE_NAME>.jks –ext
SAN=dns:<SITE_NAME>
```

3. In the command above, <SITE_NAME> is the name of the Keystore generated in earlier section and <ALIAS> is the name of the entry in the Keystore that defined in earlier section. The CSR will manifest itself as an output file based on the Certificate Info you entered earlier. You will also need to enter the Keystore password to proceed.
4. The CSR output file is in the same current working directory, for example, <SITE_NAME>.txt.

Backing Up the Keystore

Save and back up the Keystore file to a safe, secure location.

Importing SSL/TLS Certificate to the Keystore

After receiving your SSL/TLS certificate from Certificate Admin, you must import the SSL/TLS Certificate file to the same Java Keystore under the same alias name (for example, alias server) used to generate your CSR. If you try to install the certificate to a different keystore or under a different alias, the import command will not work.

> **Note**
>
> Before importing the SSL/TLS certificate, make sure the certificate chain is in the proper format and valid. You can use OpenSSL tool to check on the validity as follows:
>
> ```
> openssl pkcs7 –print_certs –in <cert_name>.p7b
> ```

1. Navigate to the directory where the Keystore was generated earlier.
2. Run this command:

   ```
   keytool -import -alias <ALIAS> -file <CERT_NAME>.p7b –keystore <SITE_NAME>.jks
   ```
3. In the command above, <CERT_NAME> is the name of the SSL/TLS Certificate. <SITE_NAME> is the name of the Keystore generated in earlier section. <ALIAS> is the name of the entry in the Keystore that defined in earlier section.
4. You will get a confirmation message that displays “Certificate reply was installed in keystore.” Type ‘y’ or ‘yes’ to proceed.
5. This will load all the necessary Certificates to the Keystore.
6. The Keystore is now ready to be used by the Tomcat/Tomcat Embedded Server.

Step 2: Create the Key Pair for SPMS API Authentication

Background

OAuth 2.0 is the user authorization mechanism used by SPMS API. It requires a generation of an asymmetric key pair to work. The asymmetric key pair is used to securely sign and read contents found in the Security token. Security of the API relies on the security token. API calls made without a valid Security token will be rejected. In detail, the security token contains a checksum. This checksum ensures that the token is not tampered with. The checksum is calculated by adding up the bytes in the security token and is signed by the private key. A third

party can check the validity of a token by recalculating the checksum, decrypting the original checksum with the public key, and comparing the two. Any differences between the two checksums indicates that the token has been tampered with.

> **Note**
>
> We provide the process below as an example. You can use other certificate manipulation tools to generate the public and private keys. Whichever tool you use, ensure that you download them from a reliable source and that the downloaded tool is security checked, virus scanned, and checksum checked. Without such due diligence, you may compromise the security of your installation.

Generating a new Key Pair using JSON Web Key Generator

1. Go to https://mkjwk.org/ for the JSON Web Key generator tool.
2. Select the **RSA** tab.
3. Select the right **Key Size** in bits, required for RSA key types. Recommended size is 2048 and above.
4. Select the **Key Use** as signature.
5. Select the **Key ID** as specify and enter any string, for example sign-rsa.
6. In the **ShowX.509**, select **No**
7. Copy the ‘Public Key’ and “Public and Private Keypair Set” into a separate files with .json extension and save.
8. Amend the ‘Public Key’ file to include the keys array as shown below:

   Sample Public key:

```
{
    "keys": [
        {
            "kty": "RSA",
            "e": "AQAB",
            "use": "sig",
            "kid": "sign-rsa",
            "alg": "RS256",
            "n": "g88SjdDsfdHd64fdf..."
        }
    ]
}
```

   Sample Private key:

```
{
    "keys": [
        {
            "p": "5BjdvhhdGjjjdsUI...",
            "kty": "RSA",
            "q": "k-7TihGsdfjnjLLf8...",
            "d": "e4t4J7dfk7jddPo78...",
```

```
                "e": "AQAB",
                "use": "sig",
                "kid": "sign-rsa",
                "qi": "UlYwJ6Jsdfsdfc...",
                "dp": "CDz5rYYsdffffI1...",
                "alg": "RS256",
                "dq": "fBAEeUP98HHdf...",
                "n": "g88SjLLjsdf881IP..."
            }
        ]
}
```

Step 3: Install Oracle Hospitality Cruise Property Management

You can perform a custom installation or a typical installation. A custom installation allows you to exclude the products that you do not need. If you choose to perform a typical installation, manually remove or disable the features that you do not need after the installation.

> **Note**
>
> If you currently have a version earlier than 23.2 installed, you must uninstall it from Windows Control Panel before installing Cruise Property Management 23.3.

Installing Oracle Hospitality Cruise Property Management

1. Log in as a Microsoft Windows Administrative user.
2. Start the installation program by right-clicking the **CruisePropertyManagement_23.3.0.exe** and select **Run as Administrator**.

Figure 7-1 Oracle Hospitality Cruise Property Management Installation – Introduction

3. Click **Next** and navigate to the "*Choose Install Folder*". The default folder is "`C:\`"

   If you choose to install it in a different folder from the default, you need to grant the folder full permission so that the user can start the APIs or Apps.

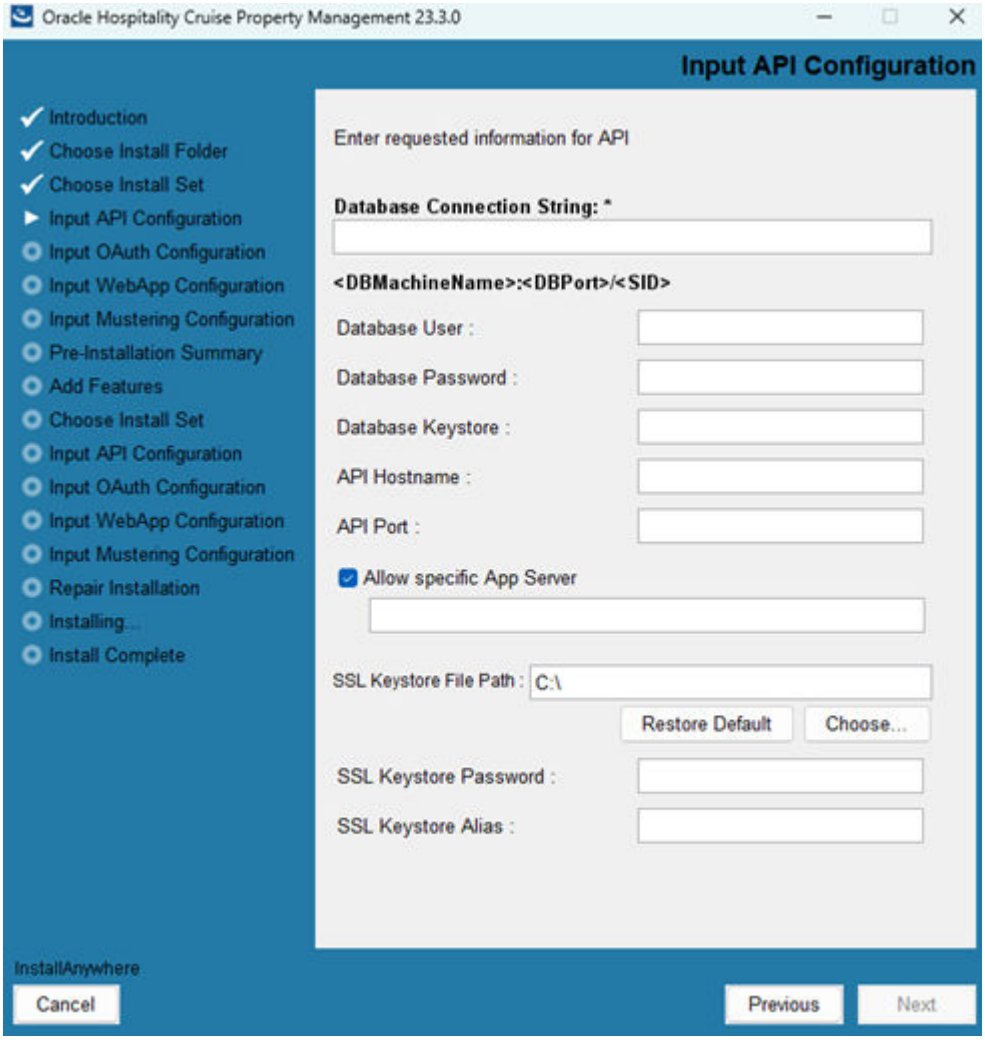
4. To grant the folder permission,
   - Access the **Properties** dialog box.
   - Select the **Security** tab.
   - Click **Edit**.
   - In the Group or user name section, select the user(s) you wish to set **permissions** for.
   - In the Permissions section, use the checkbox to select the appropriate **permission level**.
   - Click **Apply**.
   - Click **OK**.

5. Click **Next** and navigate to "*Choose Install Set*" and if you choose,
   - **Typical**, install most common application. This option is recommended for most users
   - **Custom**, selection of features to install based on the requirements

> **Note**
>
> To use the Mustering application, you must install the WebApps.

6. Click **Next** to input the fields for Input API Configuration. All fields are mandatory.

Figure 7-2 Oracle Hospitality Cruise Property Management Installation – Input API Configuration



- **Database Connection String:** <DBMachineName>:<DBPort>/<SID>
- **Database User:** Database user name.
- **Database Password:** Database Password.
- **Database Keystore:** Database Keystore's to encrypt Database Password. Minimum password length is 14 characters.
- **API Hostname:** API Server's Hostname.
- **API Port:** API Server's port number.

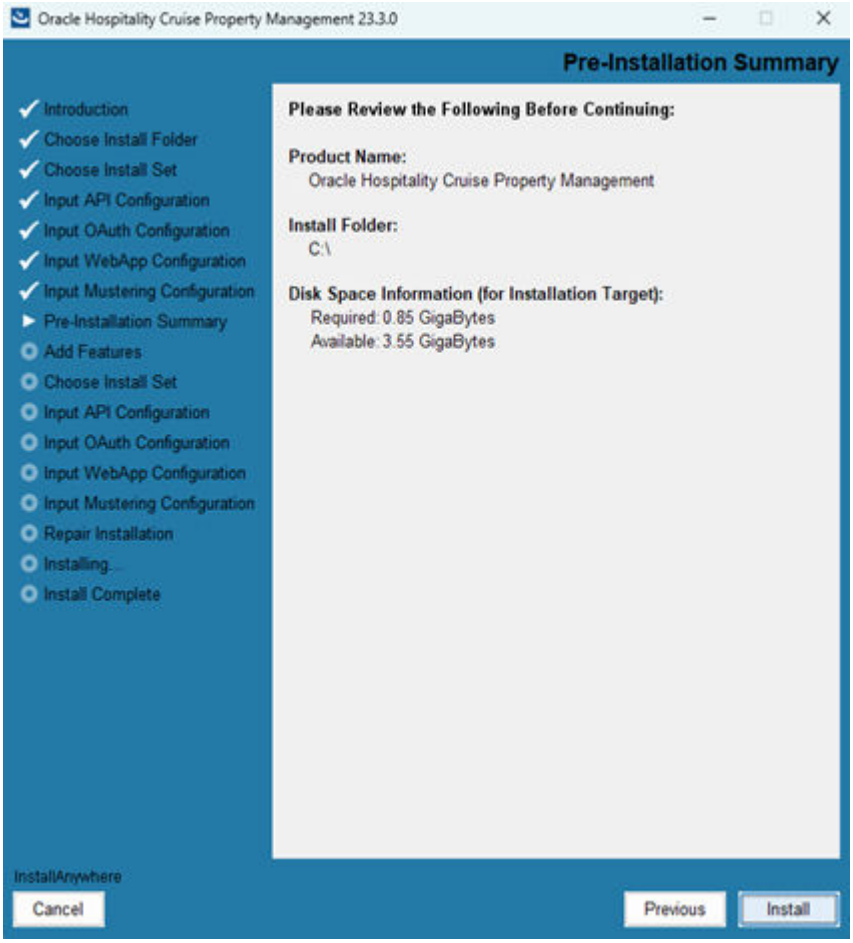
- **Allow specific App Server:** Check to enable input of server machines with APP installed that are allowed to access the API. Uncheck if it apply to all servers.
- **SSL Keystore File Path:** Choose a Keystore file in Java Keystore (JKS) type. The **Restore Default** button will reset the directory used in previous installation.

> **Note**
>
> You need to ensure that the 'Users' group in the folder's Properties under the Security tab has full access.

- **SSL Keystore Password:** Keystore password.
- **SSL Keystore Alias:** Private key/Alias used to generate the keystore.

7. Click **Next** to input the OAuth Configuration
   - **OAuth Public Key File:** OAuth public key file in .json file extension.
   - **OAuth Private Key File:** OAuth private key file in .json file extension.
8. Click **Next** to input the Web Application Configuration
   - **WebApp Port**: Single instance of WebApp port is supported. User need to choose an unused port for the installation.
   - **API Gateway**: By default, it is based on the API Hostname and port number defined in earlier step. However, if the API is located at another server, user need to define the installed API server name.
   - **SSL Keystore File Path:** By default, it is based on the Keystore File path that defined in earlier step. If a different WebApp server is present, choose the right keystore file path.
   - **SSL Keystore Password**: By default, it is based on the Keystore Password that defined in earlier step. If a different Keystore file is present, kindly enter a different Keystore Password.
9. Click **Next** to input Mustering Configuration
   - **Mustering Port**: Single instance of Mustering port is supported. User need to choose an unused port for the installation.
10. Click **Next** for Pre-Installation Summary and verify that it is the desired set up.

Figure 7-3 Pre-installation Summary



> **Note**
>
> The Install Folder shown in the summary refers to the folder directory. Disk Space Information shown indicate the disk space required for the installation. To ensure a successful installation, do ensure that the computer has sufficient disk space.

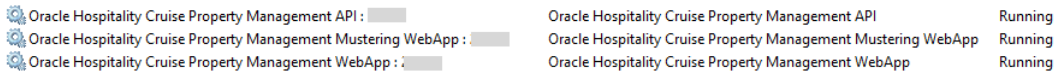
11. Click **Install** to begin installation.

> **Note**
>
> For a better end user experience, at the end of the installation a installer.properties file containing all the configurations, encryption of passwords is created and added to folder where the Cruise Property Management InstallAnyWhere is placed. The installer.properties file's content will be reset once the InstallAnywhere application is triggered. If you would like to maintain the same configurations or information, please backup this file.

12. At the end of the installation, the system creates three (3) new Windows Services and they are:
    - **Oracle Hospitality Cruise Property Management WebApp,**

- **Oracle Hospitality Cruise Property Management Mustering WebApp** and
- **Oracle Hospitality Cruise Property Management API**.

and the corresponding programs will be placed under `[InstallationDir]\Oracle Hospitality Cruise\Property Management`



> **Note**
>
> If it is needed, you can change the background picture of the Cruise Property Management or Mustering application login page by replacing the PNG file located at their respective folders.
>
> For the Cruise Property Management login page, go to `[InstallationDir]\Property Management\v23.x\WebApp\instances\WebApp_[Port Number]\webapps\ROOT\signin\styles\dynamicImages\2f16834fca12fd6d8f35.png`
>
> For the Mustering application login page, go to `[InstallationDir]\Property Management\v23.x\WebApp\instances\MusteringApp_[Port Number]\webapps\ROOT\signin\styles\dynamicImages\2f16834fca12fd6d8f35.png`

Modifying / Uninstalling Oracle Hospitality Cruise Property Management

Any modification or uninstallation are done through Windows Control Panel in a Maintenance mode. This would allow user to select the options to perform like add features, remove, repair or uninstall the product.

1. Start the installation program by right-clicking the **CruisePropertyManagement_23.3.x.exe** and select **Run as Administrator**.

   If you have already installed the application, the Setup would start in Maintenance mode. Choose one of the options presented.

   - **Add Features:** InstallAnywhere will guide you through adding features to the installed set. The feature will be disabled if it is already installed.
   - **Remove Features:** InstallAnywhere will guide you through removing features of the installed product. User can *uncheck* the product features (WebApp / API /Mustering) that need to uninstall. Checked features will remain installed.
   - **Repair Product:** This function repairs the features of installed product and checks if API services are installed. If API Services are installed, the Database Connection settings screen appears, prompting you to enter the API DB Password.

     The installer automatically encrypts the password before replacing the old password with the new, encrypted password, updates the configuration and restart the API service with the new password.

     If the API Services are not installed, the installer exists and display *“API is Not Installed. Repair installation is only available for the API feature.”*

- **Uninstall Product:** InstallAnywhere will remove all the features that were installed during product installation. Files, folders and windows services **will** also be removed.

2. Click **Next/Uninstall** and follow the wizard instructions.

Upgrading Oracle Hospitality Cruise Property Management

If you already have a previous installation, follow these steps to upgrade the program. You would need an Administrative privilege to perform this task.

1. Locate the `installer.properties` file in the previous installation folder.
2. Copy the `installer.properties` file into the folder where latest **CruisePropertyManagement_23.3.x** installer is located. This is to ensure the previous settings like database connections, installation paths, and other configurations are retained.
3. Start the installation program by right-clicking the **CruisePropertyManagement_23.3.x.exe** and select **Run as Administrator**. The data of previous setup will pre-populate when the condition above is met.
4. Click **Upgrade** to begin and follow the instructions on screen.
5. At the end of the installation, the previously installed version is replaced with the latest features, fixes, and updates included in this release.

Downgrade Prevention:

Installing a lower version over SPMS 23.3.x is not permissible once the program is upgraded to SPMS 23.3.x or later. The system will prompt a notification to terminate the installation.

8
Verifying SPMS Setup

After installing all necessary SPMS components, verify the SPMS setup to ensure every component works as intended.

Verifying SPMS Secure Server

1. On one of the SPMS Application Client machines, navigate to its SPMS Public Document folder `C:\Users\Public\Documents\Oracle Hospitality Cruise`.
2. Backup and remove the Secure Credential file from the SPMS Application Client machine.

> **Important**
>
> Do not remove the Secure Credential file from the SPMS Secure Server.

3. Navigate to the SPMS Installed Folder `C:\Program Files (x86)\Oracle Hospitality Cruise`.
4. Locate the file SecureLogin.txt.
5. Set the IP address or machine name of the SPMS Secure Server as the content of the SecureLogin.txt.
6. Attempt to log in to the OHC Launch Panel from the same SPMS Application Client machine. If the SPMS Secure Server is working as intended, you will see a new local Secure Credential file on the same SPMS Application Client machine, and the login to the OHC Launch Panel will be successful.

Verifying SPMS Webservices

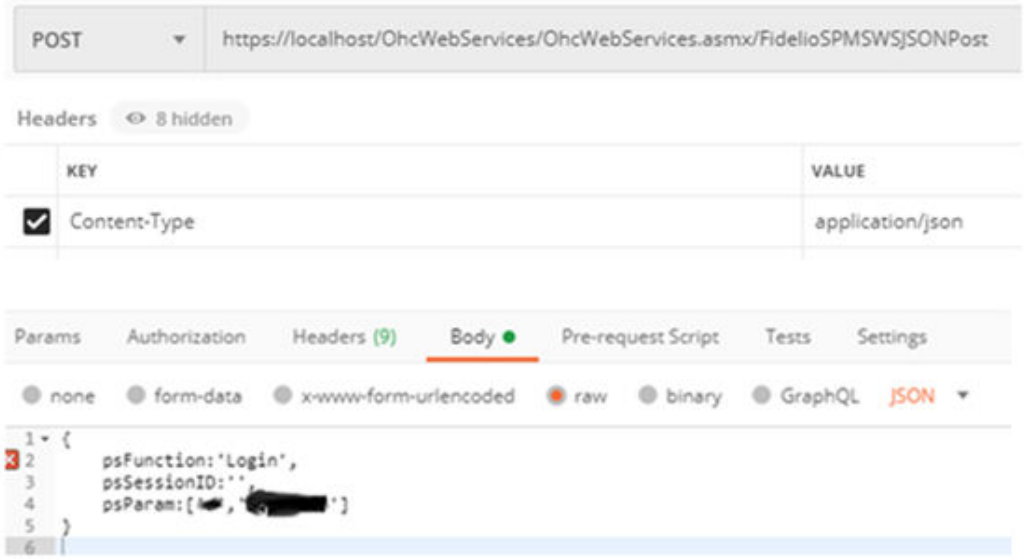
1. From the SPMS Web Server, navigate to `C:\inetpub\wwwroot\OHCWebServices` folder.
2. Check the web.config file to ensure that the SecureLogin points to the correct SPMS Secure Server.

```
 <appSettings>
        <add key="Server" value = "<DB_TNS_NAME>" />

<add key = "SecureLogin" value = "<SECURE_SERVER_NAME>" />
</appSettings>
```

3. Test an SPMS login command by using POST method with JSON structure.

Figure 8-1 POST Method with JSON Structure



4. If you can log in successfully, this means the SPMS web services is hosted correctly and able to connect to SPMS Database.

A

Appendix

Oracle Database Client and ODAC Installation

SPMS Application Clients and SPMS Web Servers are database clients. They need to connect to the SPMS Database to operate. As such, the installation of Oracle Full Client and ODAC setup is required.

Where to download Oracle Database Client

1. For instructions, download a copy of the installation manual from the official Oracle Help Center website at https://docs.oracle.com/en/database/ and refer to the manual for steps to install.
2. Similarly, to install the Oracle Database Setup file, refer to the website at https://www.oracle.com/database/technologies/instant-client/downloads.html and download the appropriate Microsoft Windows installation file.
3. Alternatively, you could obtain a specific setup file from Oracle Support/DBA. For example, these are some of the installers made available:
   - Oracle Client 19c

How to register Oracle Database Client DLLs to the Local Environment

The Oracle Database Setup file downloaded from the Oracle website will not automatically register the above DLLs to the local client. Oracle provides a tool (OraProvCfg.exe) to help you to register the DLLs.

For example:

- Navigate to `%ORACLE_CLIENT_HOME%\ODP.NET\bin\2.x`.
- Run the following command: `oraprovcfg.exe/action:gac/providerpath:Oracle.DataAccess.dll`

The specific Setup file from Oracle Support/DBA will normally register DLLs automatically.

For SPMS to be able to connect to the Oracle Database, the Oracle Database Client DLLs must be registered to the local client. The DLLs that must be registered are:

- Oracle.DataAccess.dll
  - Folder: `ORACLE_HOME\odp.net\bin\2.x`
- All DLLs under PublisherPolicy folder: Policy.X.XXX.Oracle.DataAccess.dll
  - Folder: `ORACLE_HOME\odp.net\PublisherPolicy\2.x`
- Oracle.ManagedDataAccess.dll
  - Folder: `ORACLE_HOME\odp.net\managed\common`
- All DLLs under PublisherPolicy folder: Policy.X.XXX.Oracle.ManagedDataAccess.dll
  - Folder: `ORACLE_HOME\odp.net\managed\PublisherPolicy\4`

> **Note**
>
> To establish a Database connection using Oracle Net Manager, use the following steps:
>
> 1. Once the Oracle Client installation is successful, launch the Oracle Net Manager to establish the connection between the Database Client and Database Server.
> 2. When installing the ODAC, ensure the following components for Oracle 19c are installed:
>   - Oracle Data Provider for .NET
>   - Oracle Providers for ASP.NET
>   - Oracle Services For Microsoft Transaction Server

Definition of SPMS Seed Database

An SPMS Seed Database is a template database imported from a suitable Database DMP file. As in SPMS 7.30 and prior, a new database setup has always been a process of importing from a suitable Database DMP by DBA and then the new database will undergo a purge process (FCSPMS_Clean_UP.SQL) to ensure the database is empty. Similarly, for SPMS 8.0 / 20.X and above, a new database template will follow the same process in SPMS 7.30. A suitable Database DMP will be chosen and then the data will be purged to ensure the database is empty.

General Troubleshooting Steps

Common Errors in SPMS Database Installation

Shown below are some of the common errors encountered during the Database Upgrade process using the OHC Tools.

For 1st time upgrade to version 20.X / 23.X using OHC Tools, program does not directly start with Upgrade screen. Login screen prompt an error 'Secure Server is not running at xxx'

- This could be due to the fact that the FIDELIOBK does not exist or the account is locked or the password is not a default password. Unlock the account or update the password manually.

Error “Unique Constraint (FIDELIO.TYP.I1)” occurs after upgrading DB to 20.X / 23.X and when running OHC Tools.

- This is because the database is yet to upgrade to version 20.X / 23.X. Run DB Installer version 20.X / 23.X.

Error “Failed to connect to Updater Scheduled Task” after running DB Installer upgrade to database to version 8.0.x and launching OHC Tools without bypass updater.

- Ensure the latest Updater.exe, UpdaterWatchdog.exe is in the Program file folder and the task scheduler is up and running. Restart the PC to allow Updater to launch and perform the update.

Error prompt “Cannot load assembly Oracle.DataAccess” when running .NET program in Windows 11.

- Ensure the .NET Framework 3.5 is enabled in Microsoft Windows Features before installing Oracle Client. If an error occurs in the Web Server, reinstall the Oracle Client after performing the Web Server Setup.

.NET Program failed to connect and error prompt “Cannot load assembly 'Oracle.DataAccess” on IIS Server with ODAC 19c installed.

- Place the 'Oracle.DataAccess.dll' into `c:\inetpub\OHCTransactionsService\bin` folder.

Message prompt “TNS: could not resolve the connect identifier specified” when running OHC Tools.

- Ensure the DB SID <> ‘Fidelio’ and OHCSettings.par exist in Public Folder or DB SID <> ‘Last Server’ in OHCSettings.par

Message prompt “TNS: could not resolve the connect identifier specified” when running OHC Tools, Change Encryption Key failed to store passphrase due to the above error.

- Ensure the IIS Server can connect to the database. Use the SQLPLUS or RESTART IIS Server to test the connection.

Message prompt “Web Service DB Server = xxx, Client Server =xxx, cannot proceed” when running OHC Tools, Change Encryption Key.

- Ensure the DB SID defined in Web.config / Tnsnames.ora / OHCSettings.par are the same as IIS Server and Client PC.

Message prompt “Invalid username/password” when the user subsequently changes the Encryption Key.

- The issue is caused by a connection time out during the encryption process and Secure Credential file were not properly created in the IIS Server. Manually remove Secure Credential file from the IIS Server and run Change Encryption Key to recreate the file.

Message prompt “Secure Server is not running at xxx” when running OHC Tools / OHC Launch Panel for the first time and it failed to connect to IIS Server.

- Ensure the IIS Server Firewall Port 443 is turned off.

Message prompt “old password does not match” when running OHC Tools, Change Encryption Key.

- The database password is case sensitive. Ensure the database password is correct. You can change the case sensitivity using an SQL statement if the error persists.

Message prompt “The path is not of a legal form” when running OHC Tools.

- The issue is caused by SYS_REPORTDIR being empty. The workaround is to place a value to this parameter or obtain the latest Fidelio*.dll.

Message prompt “Unable to launch application due to invalid fideliobk, system cannot determine current db is 7.30.8xx or 8.0.xx” when running OHC Tools.

- The issue might be caused if the schema created uses the wrong password when backing up and restoring the database. Manually drop the FIDELIOBK from the schema.

Warning “Error code [E730878] detected during DB verification. Please contact Oracle Support.” after running the DB Installer.

- This warning indicates the minimum database version (7.30.878 or 8.0.12) was not run prior to upgrading to 20.X. See Prerequisites in *Setting Up SPMS Database Server*.

Common Errors in SPMS .NET Web Server Installation

Web Server Is Corrupted

If the SPMS web services server is corrupted, the Secure Credential file is no longer valid.

Set up the new IIS Server and connect to the new IIS Server using an existing client PC.

1. Ensure the Secure Credential file exist on the client PC.
2. Change the securelogin.txt to point to the new IIS Server.
3. Run **OHC Tools, Change Password** function to generate a new key.

Logged in user changed or the user does not exist in Secure Credential file.

- Run **OHC Tools, Change Password** and perform a password change to copy all of the entry with value in Secure Credential file to new IIS Server, then log in to SPMS application on a different client PC to download Secure Credential file from IIS Server.

Message prompt “The Operation is complete but NetFx3 feature was not enabled” when installing Web Service, Enabling Features.

- Log in to the IIS Server with a user from an administrator group instead of the standard user group, and restart the installation.

Error prompt “Certificate error” when browsing the TransactionsService using Internet Explorer.

- A secure certificate is not present in your environment. You are required to purchase the certificate from a certificate authority and apply the said certificate. For more information on how to apply a security certificate, see https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/a2f35fcd-d3b6-4f39-ba93-041a86f7e17f.mspx?mfr=true.

Message prompt “TNS: listener does not currently know of service requested in connect descriptor”.

- Ensure the Database is up and running.

Message prompt “Fidelio user password for server xxx not found”.

- This error is caused by Secure Credential file being manually deleted and the application already connects to DB, and is comparing the old password with IIS Server. Restart the IIS Server to enable the application to re-establish its connection.

Wrapper.dll not registered.

- Launch the MS-DOS Command with “Run as Administrator” and use RegAsm in `C:\Windows\Microsoft.NET\Framework\v.4.0.30319` to register the Wrapper.dll file.

Message prompt: “The Specified method not found.”

- The system prompts this message when the user attempts to load the .asmx file through Internet Explorer. Some of the DLL should not exist in the BIN folder, for example. SingPlusNet.dll. Remove them and retry.

Error Message: ‘Unhandled exception has occurred in your application. System.MissingMethodException: Method not found’

- This occurs when App_Code.dll, OHCSPMS*.dll version is wrong. Ensure these DLL versions are the same.

Error Message: “Critical error occurred while processing Sql statement.\r\n. Please call your system administrator, application will terminate now or .Error Message: Oracle.DataAccess.Client.OracleException ORA-06576: not a valid function or procedure name at Oracle.DataAccess.Client.OracleException.HandleErrorHelper.”

- This occurs when logging in to JSONGet. Ensure both OHCSPMS*.dll versions are the same as the Database version.

Error Message: “Critical error occurred while processing SQL statement.\r\n Please call your system administrator, application will terminate now.\r\n\r\nSystem.Exception: Error Opening Connection to - Unable to load OraMTS….”

- This occurs when performing a transaction through Oracle WebServices. Ensure the Oracle Services for Microsoft Transaction Server (MTS) is installed on the Web Server.

Error Message: “Critical error occurred while processing SQL statement. Please call your system administrator, application will terminate now. System.Exception: Error Opening Connection to – Unable to enlist in a distributed transaction …….”

- This occurs when running Infogenis Point-of-Sale (IGPOS). Install ODAC and ensure the MTS is enabled and running properly as well as the distributed transaction coordinator service.

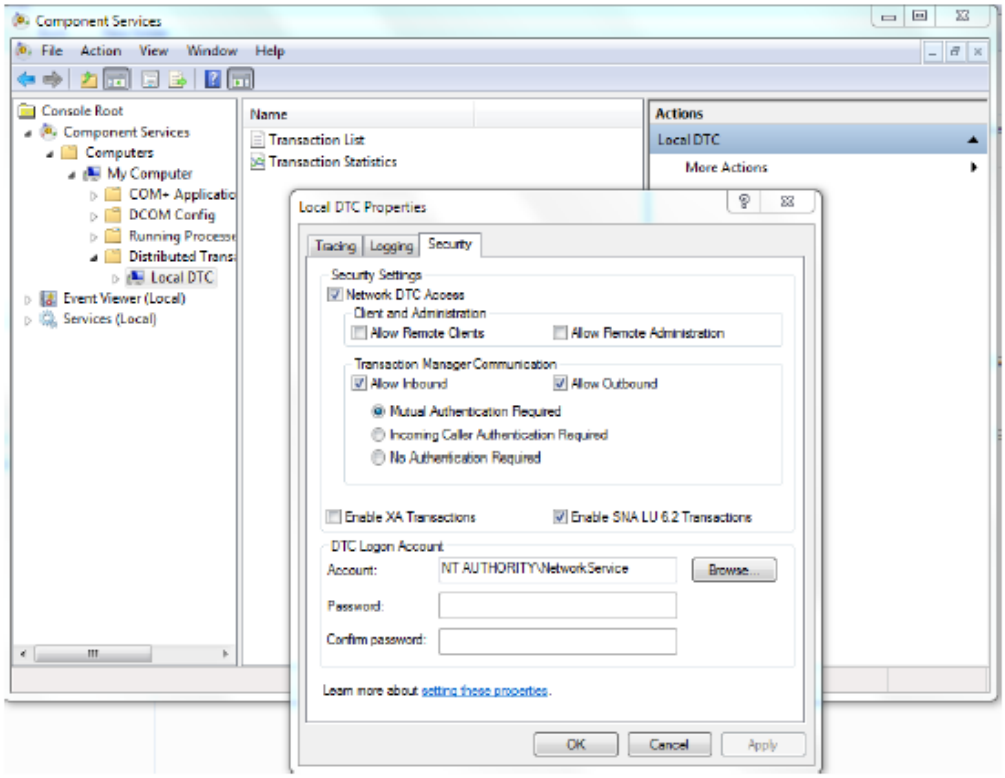
Error Message: “OHCSPMSxxxx.DLL Version (xx.xxx) does not match with….”

- The error occurs when running IGPOS. Ensure the OHCSPMS*.dll version in XAPP table is as the copy in the BIN folder.

Error Message: “penConnection-System.InvalidOperationException: The Promote method returned an invalid value for the distributed transaction.”

- This error occurs when performing a web service transaction like Check-In or Book Excursion. In the Component Services, Distributed Transaction, Load DTC Properties, Security tab, and select both the ‘Allow Inbound and Allow Outbound checkbox.

Figure A-1 Windows Component Services



Issue with: Web Browser showing “Page Not Found.” Error 404 – File or Directory not found.

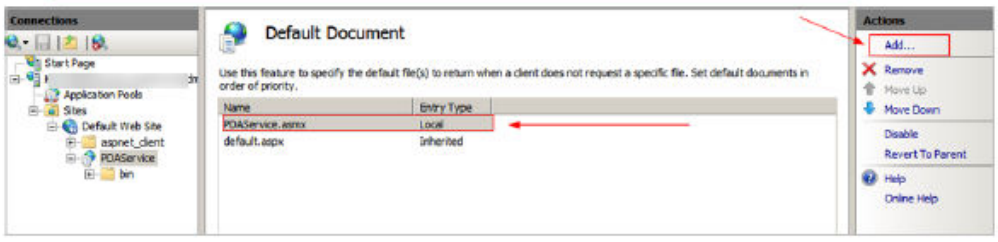
- Ensure the IIS, WebService Extensions are set to **Allowed** in Web Service Extensions.

Issue with: Web Browser showing blank page when browsing the OHC Webservices, or error “The Specified module could not be found.”

- This error occurs when testing the web service through Internet Explorer and it returns a blank page.

  1. Navigate to the IIS Manager and select OHCWebServices.
  2. In the Default Document, manually add the OHCWebServices.asmx file.

Figure A-2 IIS Manager - Default Document

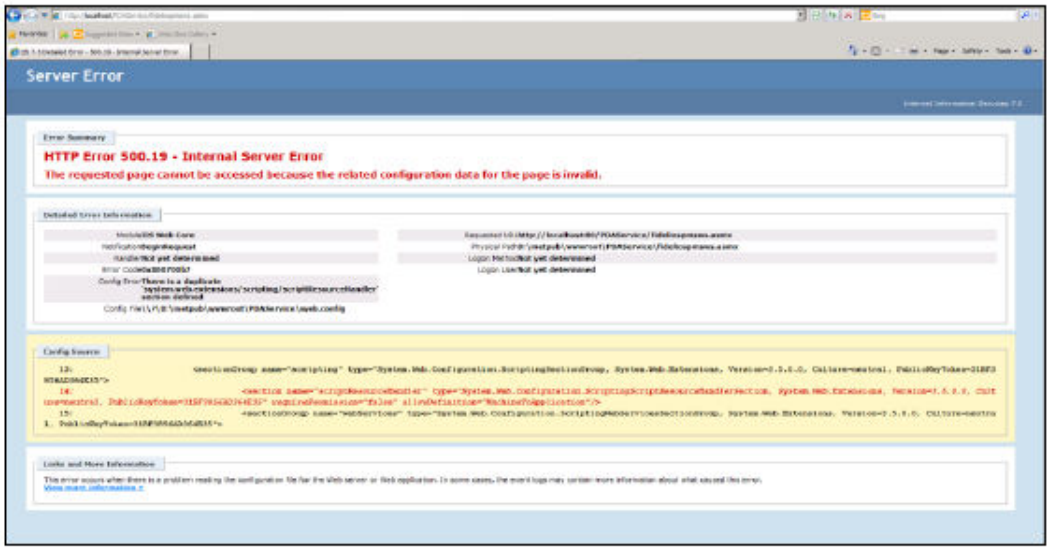


Error Message: “This setup requires Internet Information Server 4.0 or higher and Windows NT 4.0, Windows 2000 or higher….”

- This error occurs during OHCWebServices Setup and requires Internet Information System (IIS) 6.0 or higher in Control Panel, Windows Features to be turned on.

Error Message: “Error Code 0x800700b7 Config Error. There is a duplicate system.web.extensions/scripting/scriptResourceHandler” section defined.

Figure A-3 WebServices Error Message



- This error occurs when browsing the web page. Comment of the related thread is mentioned in web.config.

Error Message: ‘<!--<sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">’ or ‘The type initializer for ‘FidelioSPMS.CShipGeneral’ threw an exception.

- This error occurs when browsing the web page. Ensure the .NET Framework version is .NET Framework v4.0.30319 in the Application Pool, Default Pool setting.

Common Errors in SPMS Desktop Application Client Installation

Login user changed or the user does not exist in Secure Credential file.

- Run OHC Tools, Change Password and perform password change to copy all entries with a value in Secure Credential file to the new IIS Server, then log in to the SPMS application on a different client PC to download the Secure Credential file from the IIS Server.

All Credit Card numbers displayed are masked.

- The issue may be due to the PC connecting to different DB, and that DB password is the same as the previously connected DB, resulting in a mismatched encryption key in Secure Credential file. Delete the Secure Credential file and re-download the file.

Message prompt “Secure IP Not Found, cannot continue” when running SPMS application.

- The issue may be caused by SPMS 8.0 application running on a database version below 8.0.x, OHCSettings.par is not found in the public folder (where SID <> Fidelio) or securelogin.txt file does not exist or invalid.

- Ensure the above files exist and are in the correct location, and the database is updated, and the <endpoint address> points to the correct web server if the above message prompts in OHCDemoApp.

If the WS server is corrupted, the Secure Credential file is no longer valid.

- Set up the new IIS Server and connect to the new IIS Server using an existing client PC. Ensure the Secure Credential file exists on the client PC. Change the securelogin.txt to point to the new IIS Server, then run OHC Tools, and use the Change Password function to generate a new key.

Interface or OHC Watchdog program failed to run and OHC UpdaterAgent keep initiating.

- Ensure the Interface program is uploaded under the Interface Files group in XAPP (XAPP_SYSTEMS_FILES =3).

Custom.dic keep downloading from XAPP when file size is 0kb in local PC.

- Run Launch Panel to auto-save the Custom.dic file into the Public Documents folder.

Message prompt “no data found” in OHC Management when performing a guest check out.

- This issue is due to the DB Installer having an issue with the conversion of Point-of-Sale (POS) table from CHAR to VARCHAR2. Ensure you do not End the task of the DB Installer during an upgrade process.

SPMS program prompts an error ‘Due to PA-DSS Compliance...’

- The issue is caused by Secure Credential file, which does not exist or does not have the security access rights to download the file. Ensure the Wrapper.dll is the latest version.

SPMS program prompts “wrong argument” when logging to a module.

- Ensure the Wrapper.dll is the correct version and is properly registered.

OHC Updater stops verifying at Wrapper.dll process.

- Ensure the Launch Panel is in XAPP table with XAPP_ID=2.

Error “Unable to initialize database connection. Please contact your System Administrator for assistance. Unable to launch application due to missing login parameters.” where Launch Panel stops at Initializing.

- This may be due to an issue with ODAC installation. Run .NET program to verify

Run VB program hit error 'Object does not support this property type'.

- `Re-register the wrapper.dll using MS-DOS Command C:\Windows\Microsoft.NET\Framework\v4.0.30319>regasm "C:\Program Files (x86)\Oracle Hospitality Cruise\wrapper.dll”.`

Error “Failed to connect to Updater Scheduled Task; trying to connect to OHC Updater” when launching OHC Launch Panel without Bypass Updater.

- The system creates a scheduled task in Task Scheduler with the Oracle Hospitality Cruise SPMS Updater. Verify that the Oracle Hospitality Cruise SPMS Updater is running in the Task Scheduler by navigating to the Control Panel, Administrative Tool, Task Scheduler.
- If the Task is not created, manually create the task by running the createtask.bat followed by runtask.bat from the Oracle Hospitality Cruise program files folder.

Message prompt "The database which has been specified….This could be because the service is too busy or because no endpoint was found…"

- This may be due to the IIS not being available. Reset the IIS or browse the IIS Server from IE to check the availability

- Ensure Port 443 is added in the Window Firewall. Try to define IP or Server Name in SecureLogin.txt.

Message prompt "Failure Open File."

- This is caused by Oracle Wallet. Ensure the Net Manager is connected to the DB successfully. Ensure the wallet folder has granted IIS_USER.

Error from WS - HTTP binding error.

- This is due to Secure Credential file is either missing or invalid.

Error “Session Expired. Invalid username and password when connect to database or web server”

- Ensure the Secure Credential file is correct in both IIS and the local client PC

Error "Fidelio The type initializer for "Oracle.DataAccess.Client.OracleConnection’ threw an exception’ when logging into the OHC Launch Panel or OHC Tools.

- Ensure checkbox "Configure ODP.NET and/or Oracle Providers for ASP.net at machine-wide level" is selected while installing ODAC.

Error "Session Expired. Error connecting to xx. Invalid username/password. Logon denied."

- Run the SQL statement to alter the case sensitivity.

Error "Failed to print board card" when using Zebra printer.

- This is due to the Crystal Report Template being ticked on the ‘No Printer’ checkbox and the Zebra printer is not configured as Windows default printer.
- To resolve this, there are 2 alternate ways:
  - Untick the ‘No Printer’ and choose the printer option as Zebra Printer from the printer list and set the Windows default printer as Zebra printer.
  - Remain the ‘No Printer’ checkbox tick, but Zebra Printer has to be the Windows default printer.

Common Errors in Cruise Property Management Installation - InstallAnywhere

An Instance Management Error prompting “Error while checking for instances” when reinstalling the Cruise Property Management InstallAnywhere.

- It is likely due to the InstallAnywhere global registry file is corrupted. This can be resolved by:
  - Locating the InstallAnywhere global registry file under `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`.
  - Backup this file before editing.

> **Important**
>
> Do not permanently delete the current InstallAnywhere global registry file. If you delete this file, you might not be able to run other product’s installation programs that are already installed in the computer.

  - Manually delete any Content Classification strings with the product name “Oracle Hospitality Cruise Property Management” in `<products>` section.

  - Run the **Cruise Property Management InstallAnywhere** and verify that you are able to proceed with the installation.

Common Errors in SPMS Mustering Web Application Installation

How to resolve browser storage limit threshold warning

- If the device browser storage threshold limit exceeded 20 Gigabytes, a warning banner will be showing on the SPMS Mustering screen. In order to prevent the storage usage reaches the maximum and impact the apps operation, you need to free up space for the device. When storage usage reaches the maximum, mustering application will not able to functional correctly and affects the offline usage. Here are the ways that you can apply to free up the device's space:
  - Uninstall unused PWA apps.
    * Press and hold on the icon of unused Apps. One second later, a popup menu will be shown. Choose "Uninstall" or "Remove" to remove the unused apps.
  - Clear the unwanted sites cookies and data. There are vary ways to do this, it depends on the device's operation system and browser.
    * After freeing up the space and storage usage goes below 20 Gigabytes, then the browser storage limit threshold warning banner will disappear.

Common Errors in SPMS REST API/Web Application

Error "Server not responding. Error 500-Please try again. If problem persists, contact your system administrator".

- Navigate to '`[InstallationDir]\Oracle Hospitality Cruise\PropertyManagement\v23.x\spms_reception_node1_xxxxx\logs`'. Open '`spms_reception_node1_xxxxx_service.out.log`' and log displays '`Error Message = ORA-00942: table or view does not exist`'.
- Run Database Installer to create table or views needed by the application.

Error "Server not responding. Error 500-Please try again. If problem persists, contact your system administrator".

- Navigate to '`[InstallationDir]\Oracle Hospitality Cruise\PropertyManagement\v23.x\spms_reception_node1_xxxxx\logs`'. Open '`spms_reception_node1_xxxxx_service.out.log`' and log displays '` Error Message = BadCredentialsException:Invalid Client Id`'.
- Client Id is not generated. Restart Oracle Hospitality Cruise SPMS Platform API to generate new Client Id.

Setting Up Load Balancer for SPMS OPI WebServices

SPMS OPI WebServices requires the load balancer to be configured with session persistence for it to work correctly.

Load Balancer Session Persistence or Session Stickiness

Session persistence or session stickiness is a method to direct all requests originating from a single logical client to a single backend web server.

Figure A-4 Without Session Persistence

Figure A-5 With Session Persistence

> **Important**
>
> As an example, we are using NGINX Plus installed on Oracle Linux as the load balancer that is configured with session persistence. You should select the right load balancer that meets your organization's security policy.

1. **Install the Load Balancer**

   Install the load balancer on the target machine. As an example, we install NGINX Plus on an Oracle Linux machine to act as a load balancer.

2. **Ensure Firewall Rules Allow HTTP/HTTPS Connection**

   Ensure that the port 80 (HTTP) and port 443 (HTTPS) are enabled and not blocked by firewall.

3. **Configure the Load Balancing Method**

   Generally, most load balancer supports load balancing mechanisms such as round-robin, least-connected and ip-hash. For SPMS OPI WebServices, we should use ip-hash load balancing mechanism.

   In an ip-hash load balancing mechanism, a hash-function is used to determine which server should be selected for the next request (based on the client's IP address).

   As an NGINX Plus load balancer example, we set:

   ```
   upstream opi {
   ip_hash;
   server <IP_ADDRESS>:<PORT>;
   server <IP_ADDRESS>:<PORT>;
   }
   ```

4. **Configure the Session Persistence**

   Session persistence means that load balancer identifies user sessions and routes all requests in a given session to the same upstream server. For SPMS OPI WebServices, we should add a session cookie to the first response from the upstream group and identifies the server that sent the response. The client's next request contains the cookie value and

the load balancer routes the request to the upstream server that responded to the first request.

```
upstream opi {
server <IP_ADDRESS>:<PORT>;
server <IP_ADDRESS:<PORT>;
sticky cookie sry_id expires=1h domain= oracle.com path=/;
}
```

Then we should configure the load balancer to first find session identifiers by inspecting requests and responses so that it learns which upstream server corresponds to which session identifier.

As an NGINX Plus load balancer example, we set the “sticky learn” directive:

```
upstream opi {
server <IP_ADDRESS>:<PORT>;
server <IP_ADDRESS>:<PORT>;
sticky learn create=$upstream_http_LogLinkID
lookup=$http_LogLinkID
zone=client_sessions:1m;
}
```