

Oracle® Payment Interface

Oracle Hospitality Cruise Shipboard Property Management System Installation Guide



Release 20.1
F33516-01
October 2020

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

ORACLE®

Oracle Payment Interface Oracle Hospitality Cruise Shipboard Property Management System Installation Guide
Release 20.1

F33516-01

Copyright ©, 2020, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Contents

Contents	3
<hr/>	
Preface	4
<hr/>	
1 Pre-Installation	1-1
<hr/>	
Supported Database Types	1-1
2 Installing OPI 20.2	2-1
<hr/>	
3 Token Exchange Handling	3-1
<hr/>	
PSP Client-Side Certificates	3-1
4 SPMS Configuration	4-1
<hr/>	
OHC OPI Web Service:	4-1
OHC OPI Daemon Service Configuration	4-1
OHC OPI Manager	4-2

Preface

Purpose

This guide explains the setup required to configure and use Oracle Payment Interface (OPI) with Shipboard Property Management System (SPMS).

Audience

This document is intended to cover the steps required to setup OPI to handle the integration with Shipboard Property Management System.

Customer Support

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

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

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

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

<http://docs.oracle.com/en/industries/hospitality/>

Table 1-1 Revision History

Date	Description
October 2020	<ul style="list-style-type: none">• Initial Publication

1

Pre-Installation

Consider the following guidelines before installing OPI with SPMS:

- SPMS Release 8.0.8 is the minimum release you can use to integrate with OPI.
- OPI 20.2 does not install a database. If you are doing a clean install of OPI, a database must be installed first.
- OPI requires jre1.8.0_191 to be installed before OPI installation.
- OPI requires at least 6 GB of free disk space, 4GB Memory and you must install OPI using a System Administrator account.
- OPI 20.2 no longer includes MySQL within the OPI Installer as it did in previous versions. The OPI now supports multiple database types.
- A database is still required to hold the OPI configuration and audit event data but must be installed separately before installing OPI.
- Root access to the database is required during the OPI installation, only to create a dedicated OPI database user, which can have a lower level of privilege than the Root user, and is used for OPI tasks once the installation is complete.

Supported Database Types

The Oracle Payment Interface Installer release 20.2 supports the following database connections:

- Oracle Database 12c
- Oracle Database 19c

Downloading the OPI 20.2 Installer

The OPI 20.2 Installer is available for download from Oracle Software Delivery Cloud, search by:

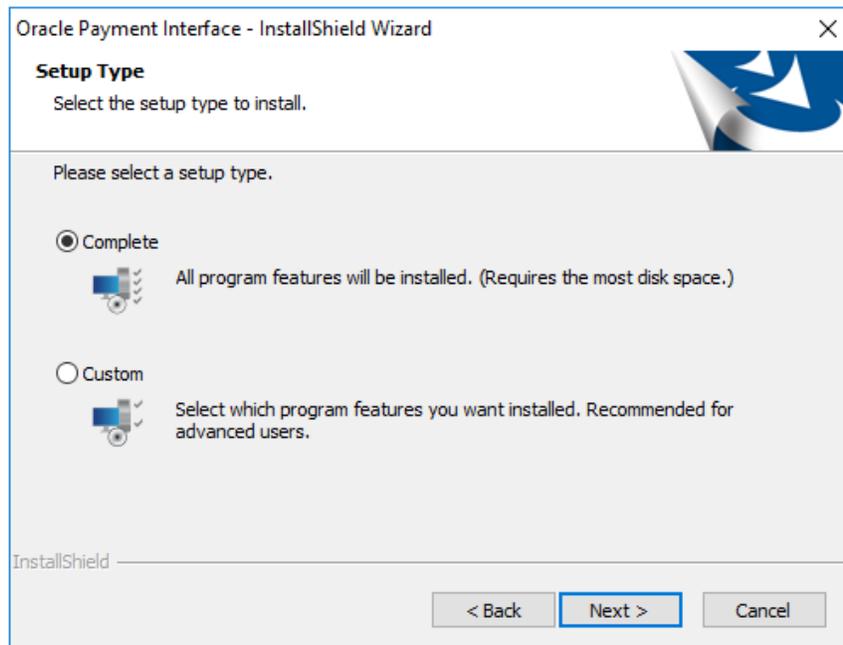
- **Release:** Oracle Payment Interface.
- **Select:** DLP: Oracle Payment Interface Without TPS 20.2
- During the installation of OPI, you must confirm the following:
 - Chain Code and Property Code.
 - IP address of the OPI Server.
 - Ensure you have the SQL root/Oracle user password for OPI database.

2

Installing OPI 20.2

1. Copy the downloaded **OraclePaymentInterfaceInstaller_20.2.0.0**, to `c:\temp` folder.
2. Right-click and select **Run as Administrator** to launch the InstallShield.
3. Select your language preference, and then click **OK**.
4. Click **Next** on the Welcome to the InstallShield Wizard for Oracle Payment Interface window.
5. Click **Next** on the OPI Prerequisites window.

Figure 2-1 - OPI InstallShield Wizard

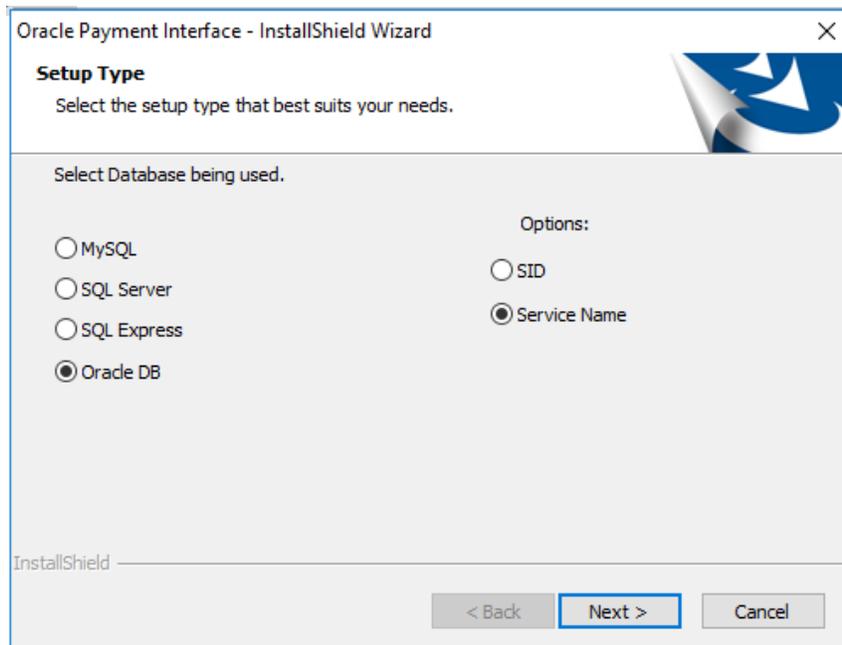


6. At the Setup Type window, select the **Complete** option to install all program features, and then click **Next**.
7. At the Choose a Destination Location window, accept the default installation location, and then click **Next**.
8. Click **Install** on the Ready to Install the Program window.
9. At the Setup Type window, select the database type used and click **Next**.

 **NOTE:**

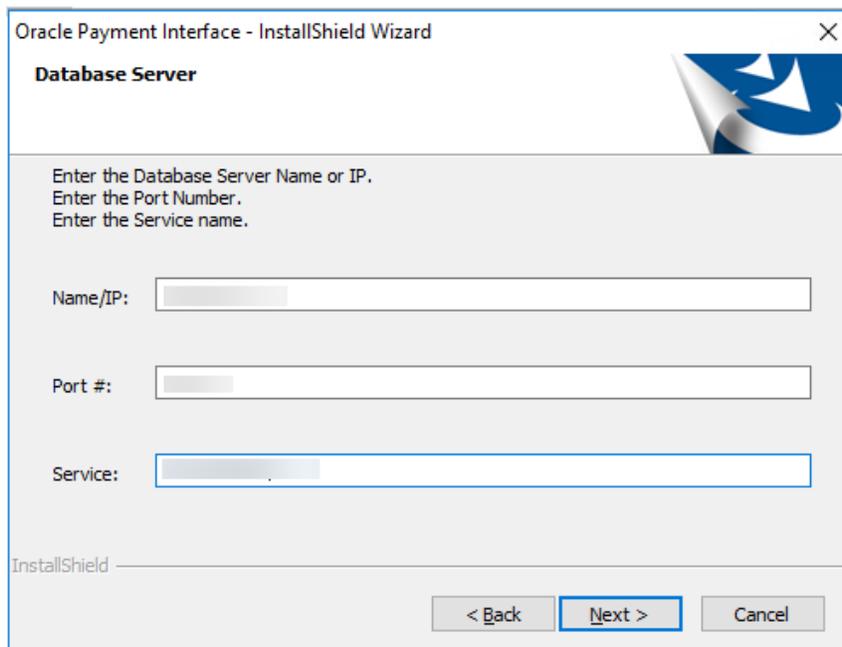
OPI does not install any database, so the database must already be installed.

Figure 2-2 - OPI InstallShield Database Selection



10. Select **Oracle DB** and **Service Name** option, and then click **Next**.

Figure 2-3 - OPI InstallShield Database Server



11. On the Server Login window, enter the DBA User credentials and then click **Next**.

Figure 2-4 - OPI InstallShield Database Server Login

The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a close button (X) in the top right corner. The main heading is "Database Server Login" and a sub-heading reads "Database server requires login credentials to continue." Below this, the text "DBA User" is displayed. There are two input fields: "Login ID:" and "Password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

12. On the Database User Credentials window, input the following and click **Next**.

- **User Name:** Create a new user.
- **Password:** Create a password.
- Confirm password

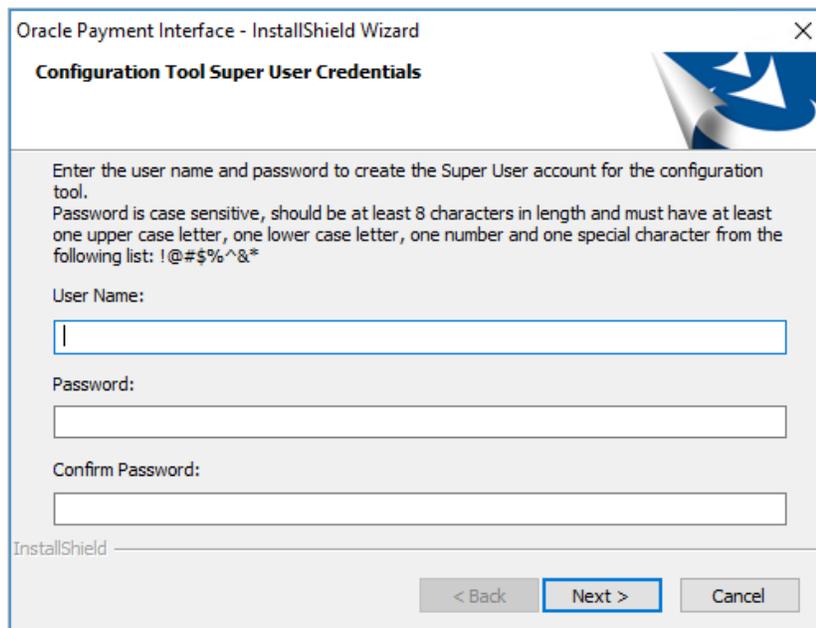
Figure 2-5 - OPI InstallShield Database User Credentials

The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a close button (X) in the top right corner. The main heading is "Database User Credentials". Below this, there is a block of text: "Enter the user name and password to create a new database user account that will be used by the Oracle Payment Interface application. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#\$%^&*". There are three input fields: "User Name:", "Password:", and "Confirm Password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

13. Click **OK** on the Database connection successful dialog.

14. The system will configure the schema and may take some time before the next prompt. Do not close the window.
15. On the Database Configuration operation successful dialog, click **OK**.
16. On the Configuration Tool Super user Credentials window, enter the following information and click **Next**.
 - **User Name:** To Create the super user account to access OPI configuration tools
 - **Password:** Create a password.
 - Confirm the password

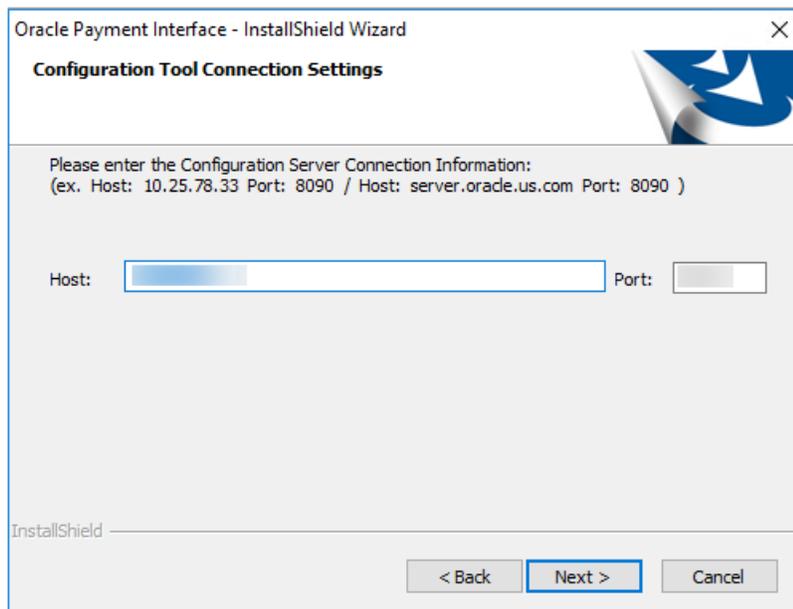
Figure 2-6 - OPI InstallShield Configuration Tool Super User Credentials



The screenshot shows a dialog box titled "Oracle Payment Interface - InstallShield Wizard" with a close button (X) in the top right corner. The main title is "Configuration Tool Super User Credentials". Below the title is a blue and white graphic of a shield with a checkmark. The main text reads: "Enter the user name and password to create the Super User account for the configuration tool. Password is case sensitive, should be at least 8 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#\$%^&*". There are three input fields: "User Name:", "Password:", and "Confirm Password:". At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog box.

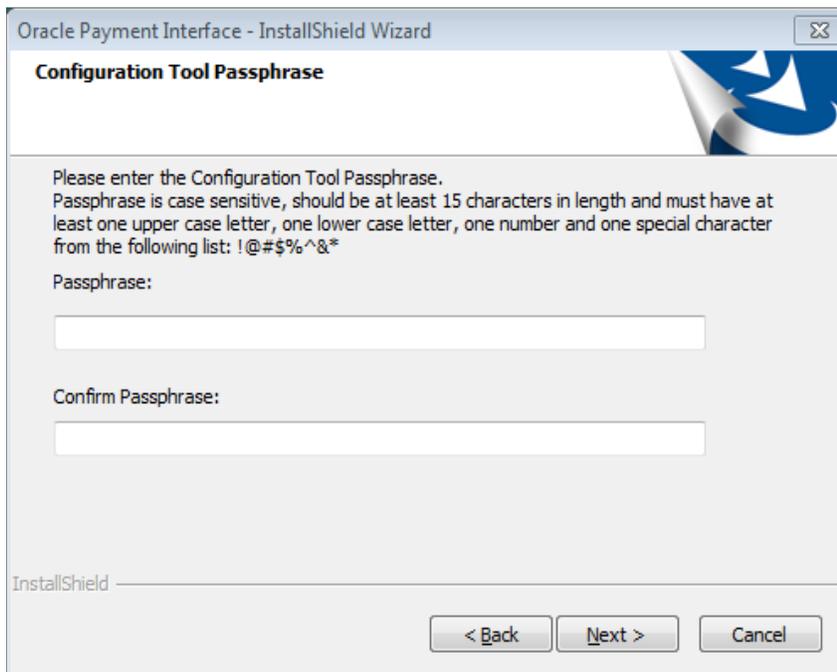
17. Click **OK** on the 'Create Super User operation successful' dialog.
18. On the Configuration Tool Connection Settings window, enter the Host IP and click **Next**.
 - **Host:** You may leave this as 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.
 - Leave the default Port as 8090.

Figure 2-7 - OPI InstallShield Configuration Tool Connection Settings



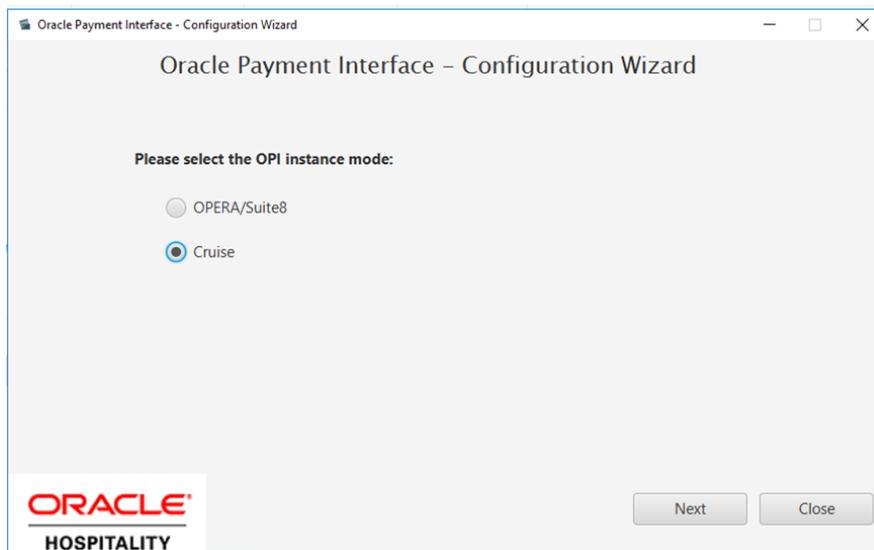
19. On the Configuration Tool Passphrase window, enter the Passphrase and click **Next**.

Figure 2-8 - OPI Install Shield Configuration Tool Passphrase



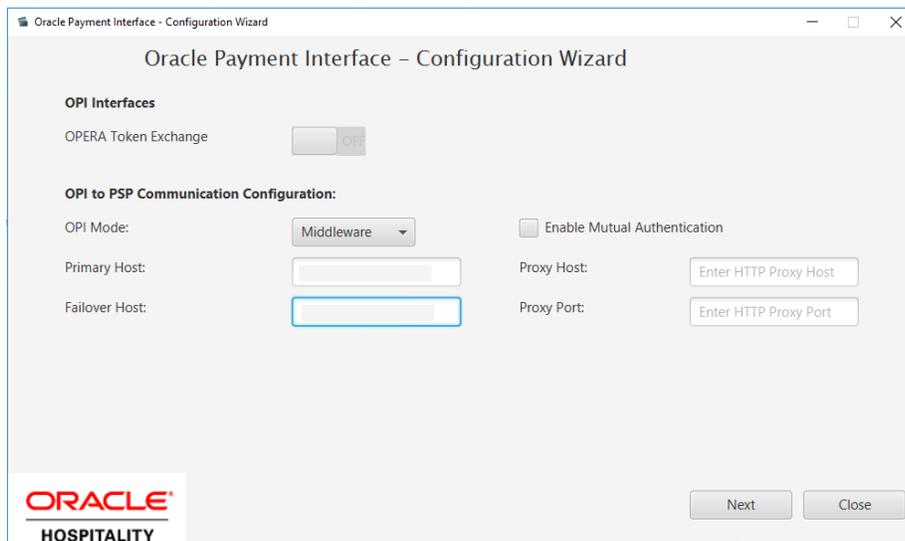
20. The following are the steps to configure OPI. At the Oracle Payment Interface – Configuration Wizard screen, choose **Cruise** and click **Next**.

Figure 2-9 - OPI Instance Mode



21. Choose Middleware as OPI Mode and fill in Primary host and Failover host under section **OPI to PSP communication configuration**.
 - a. **Select OPI Mode:** Middleware
 - b. **Set Primary Host:** Specify the middleware server information.
 - c. **Set Failover Host:** Specify the failover middleware server information.

Figure 2-10 - OPI – Communication Type



- **Host:** You may leave this as 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.
 - Leave the default Port as 8991.
22. Click **Next**.

23. On the PMS Merchant window, click the green (+) button and input the following, then click **Next**.
 - a. **Chain Code:** SPMS Chain code for the Merchant.
 - b. **Property Code:** SPMS Property code for the Merchant.
 - c. **Name:** Name of the Merchant.
 - d. **City:** City location of the Merchant.
 - e. **State or Province:** State or Province location of the Merchant.
 - f. **Country:** Country location of the Merchant, this will indicate which currency it will operate when selected.
 - g. **IFC8 Key:** This key will be inserted into OHC OPI Daemon for validation between OPI with SPMS.
 - h. **IFC8 Host:** OHC OPI Daemon machines Hostname or IP Address.
 - i. **IFC8 Port:** OHC OPI Daemon port number.

Figure 2-10 - Register PMS Merchant

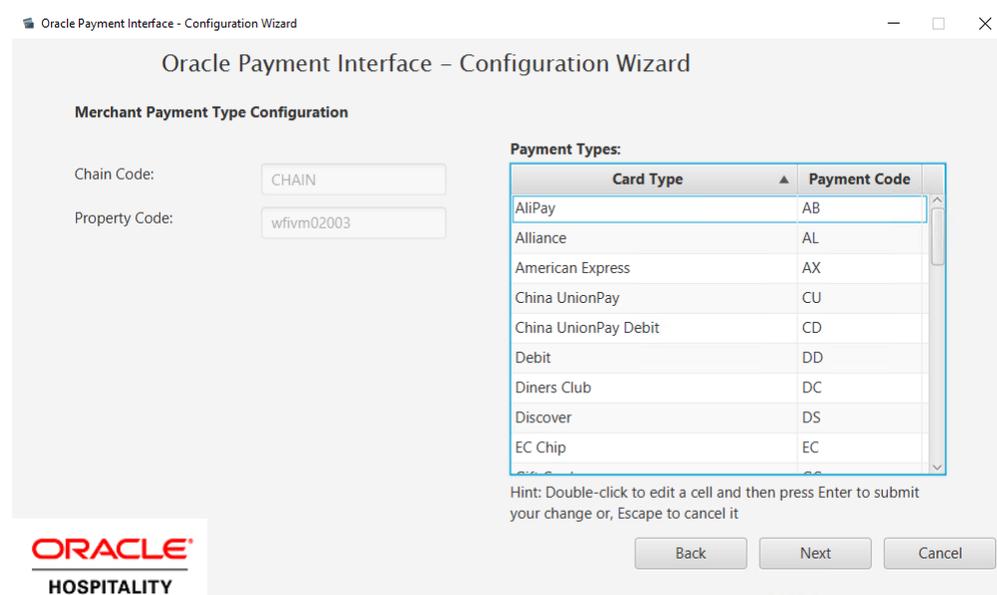
The screenshot shows the 'Oracle Payment Interface - Configuration Wizard' window. The title bar reads 'Oracle Payment Interface - Configuration Wizard'. The main window title is 'Oracle Payment Interface - Configuration Wizard'. The form is titled 'PMS Merchant' and contains the following fields and controls:

- Chain Code:
- Property Code:
- Name:
- City:
- State/Province:
- Country/Region:
- Currency:
- IFC8 Key:
- IFC8 Host IP:
- IFC8 Host Port:
- Only Do Refund

At the bottom left is the Oracle Hospitality logo. At the bottom right are 'Next' and 'Cancel' buttons.

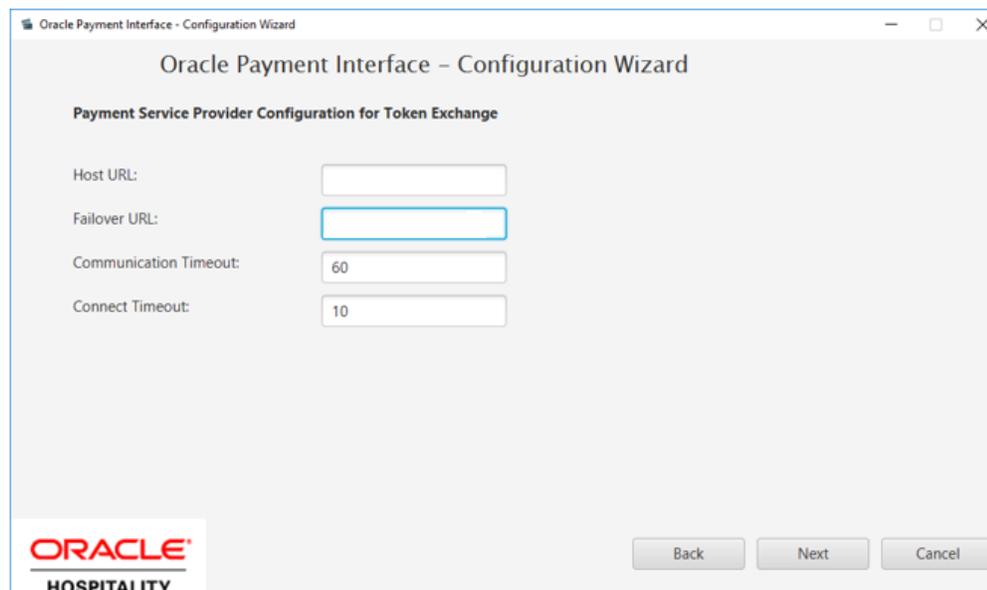
24. On the Merchant Payment Type Configuration window, the payment type accepted is shown. Click **Next** to proceed.

Figure 2-13 - Merchant Payment Type Configuration



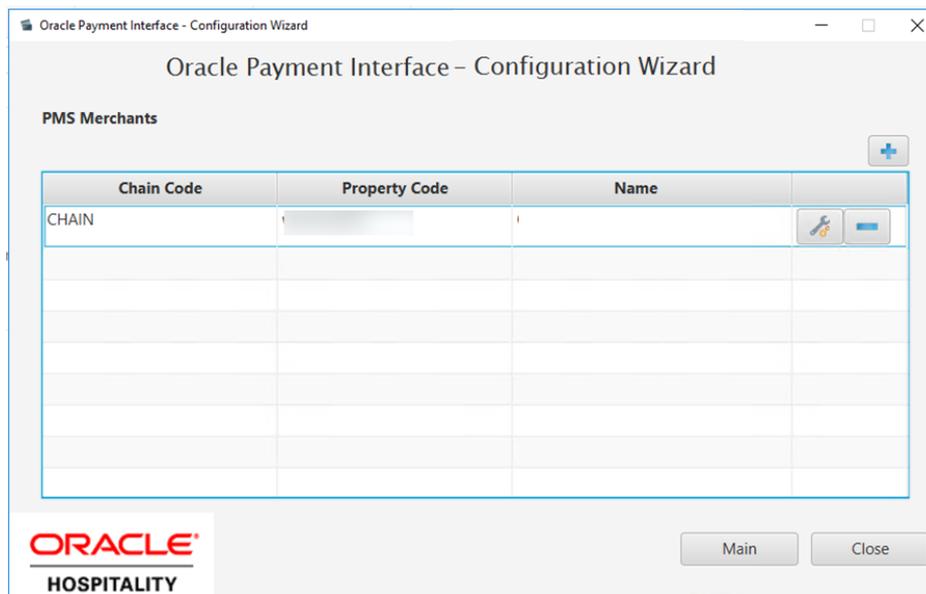
25. At the Payment Service Provider Configuration for Token Exchange window, fill in the details and click **Next**.
 - a. **Set Host URL:** Specify the middleware server information.
 - b. **Set Failover URL:** Specify the failover middleware server information.
 - c. **Set Communication Timeout:** Default to 60 seconds
 - d. **Set Connect Timeout:** Default to 10 seconds.

Figure 2-11 - Payment Service Provider Configuration

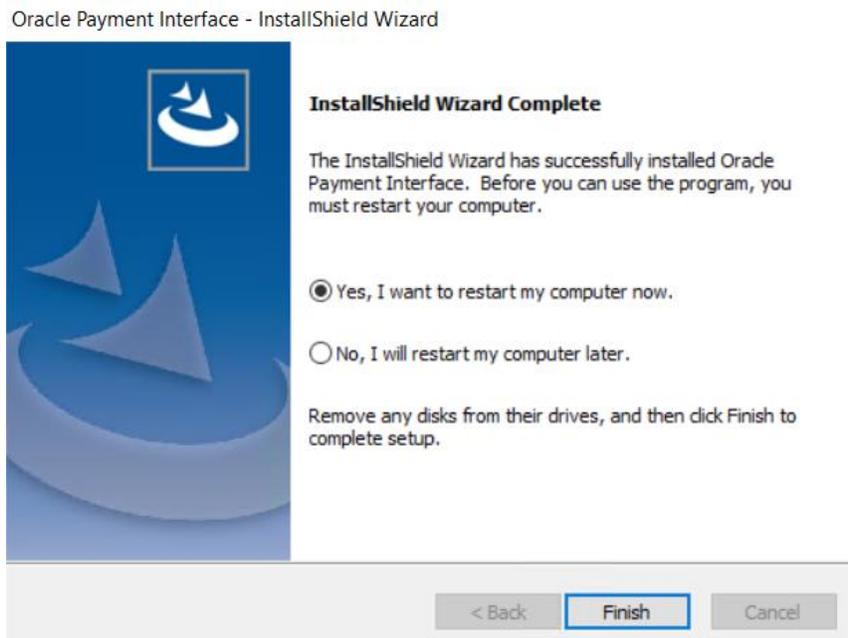


26. At PMS Merchant window, verify that the PMS Merchant is created successfully.

Figure 2-12 - PMS Merchants



27. Restart the machine when InstallShield Wizard complete.



NOTE:

The OPI installer saves detailed upgrade logs in the OraclePaymentInterface_TempLogs folder on the OPI drive. You can delete this folder if it is not needed.

3

Token Exchange Handling

This section described the settings required for token exchange handling between OPI and SPMS.

The Payment Service provider will need to provide the PSP root certificate and the client certificate.

PSP Client-Side Certificates

The communication from OPI to the PSP for token exchange uses HTTPS with a client certificate for client authentication. That is, while a server-side certificate is expected to be deployed at PSP (server-side) for HTTPS communication, PSP is also expected to provide a client-side certificate to be deployed at OPI side. OPI will present this client certificate during HTTPS communication with PSP so that PSP can authenticate OPI properly.

To achieve this, the PSP is required to provide two files:

- A client-side certificate file in the name of “OPI_PSP_1.pfx”, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. If the file provided by PSP has a different name, rename to “OPI_PSP_1.pfx” before deploying it to OPI.
- The root certificate file for the server-side certificate that is deployed at the PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server-side certificate deployed at the PSP side. We expect the root certificate file provided by PSP to be in the format of .cer or .crt. For the demo purpose in this document, we assume the file has the name “ca-cert.crt”

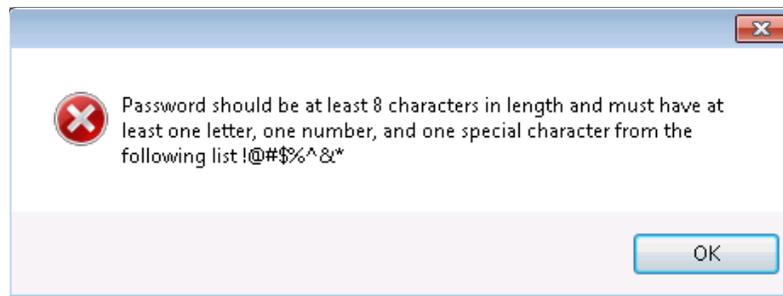
Handling the Client-Side Certificate

To deploy the client certificate on the OPI side, place the file in folder
`\OraclePaymentInterface\v20.1\Services\OPI\key\`

The passwords set by the PSP must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration.

NOTE:

The PSP Client-Side Certificates expiration date will vary depending on what the PSP set during the creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.



Handling the Root Certificate File

To load the root certificate file for the PSP server certificate into the Java key store, perform the following steps:

Creating a JKS

From a command prompt, change to the JRE bin folder for the keytool command to be recognized.

The exact path of your JRE bin folder will depend on the environment which you are running the commands and the JRE version you have installed. For example,
C:\Program Files\Java\jre1 .8.0_111\bin

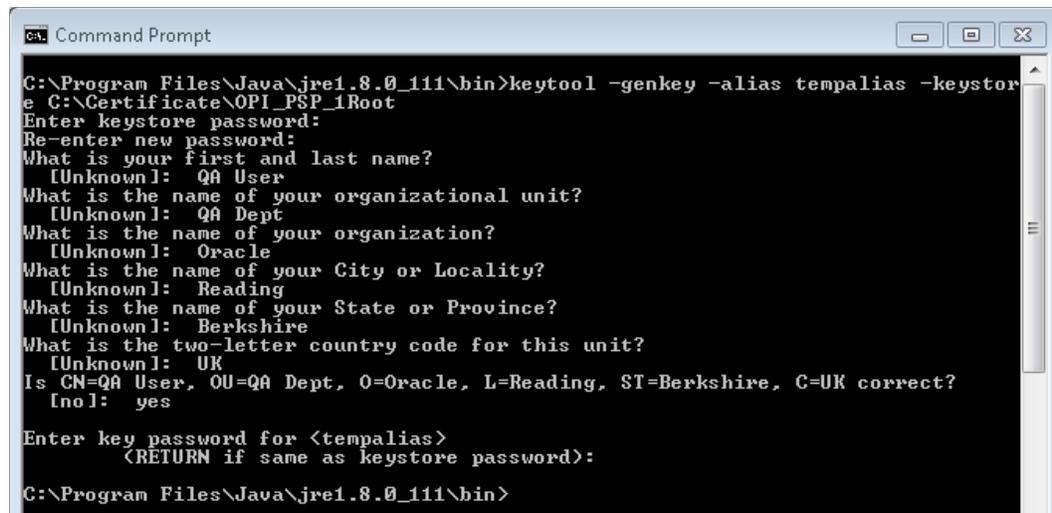
The three (3) commands below when runs in sequence;

- Create a new Java keystore,
- Delete the default key created inside the Java Key Store
- Import the supplied root certificate in its place:

In the following example, the root .cer / .crt file is named ca-cert.crt, and is located in the folder C:\Certificates. Adjust file names and paths to be relevant to your details. OPI expects that the Java key store file that contains the root certificate for the PSP server certificate to be in the name of "OPI_PSP_1Root".

```
keytool -genkey -alias tempalias -keystore  
C:\Certificates\OPI_PSP_1Root
```

You must supply some basic information during the creation of the Java keystore, including a password when prompt.



```
C:\Program Files\Java\jre1.8.0_111\bin>keytool -genkey -alias tempalias -keystore C:\Certificate\OPI_PSP_1Root
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  QA User
What is the name of your organizational unit?
  [Unknown]:  QA Dept
What is the name of your organization?
  [Unknown]:  Oracle
What is the name of your City or Locality?
  [Unknown]:  Reading
What is the name of your State or Province?
  [Unknown]:  Berkshire
What is the two-letter country code for this unit?
  [Unknown]:  UK
Is CN=QA User, OU=QA Dept, O=Oracle, L=Reading, ST=Berkshire, C=UK correct?
  [no]:  yes

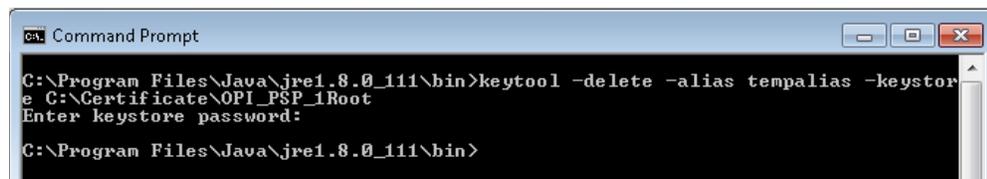
Enter key password for <tempalias>
  (RETURN if same as keystore password):

C:\Program Files\Java\jre1.8.0_111\bin>
```

You should use the same key password as for the keystore password when prompted.

For example, (RETURN if same as keystore password – Press Enter)

```
keytool -delete -alias tempalias -keystore
C:\Certificates\OPI_PSP_1Root
```



```
C:\Program Files\Java\jre1.8.0_111\bin>keytool -delete -alias tempalias -keystore C:\Certificate\OPI_PSP_1Root
Enter keystore password:

C:\Program Files\Java\jre1.8.0_111\bin>
```

```
keytool -import -alias myrootca -file C:\Certificates\ca-cert.crt -keystore C:\Certificates\OPI_PSP_1Root -trustcacerts
```

```

C:\Program Files\Java\jre1.8.0_111\bin>keytool -import -alias myrootca -file c:\
certificate\ca-root.crt -keystore C:\Certificate\OPI_PSP_1Root -trustcacerts
Enter keystore password:
Owner: CN=MerchantLink UAT Certificate Authority, OU=MerchantLink Security, O=Me
rchantLink LLC, C=US, EMAILADDRESS=edresner@merchantlink.com
Issuer: CN=MerchantLink UAT Certificate Authority, OU=MerchantLink Security, O=M
erchantLink LLC, C=US, EMAILADDRESS=edresner@merchantlink.com
Serial number: F75660745438ad3c9607277da157f94
Valid from: Thu Nov 13 19:41:15 GMT 2014 until: Wed Nov 13 19:41:15 GMT 2024
Certificate fingerprints:
    MD5:  03:C8:F1:FB:8F:31:62:51:0C:78:9E:A0:05:EE:45:C3
    SHA1: E0:78:6D:D7:B6:CB:68:0D:33:6E:0A:FD:86:0E:D1:CA:28:19:D0:D5
    SHA256: B1:5E:32:60:94:F7:8B:08:2C:33:AA:A1:A5:C5:64:24:2D:1F:F4:CC:7C:
AD:A2:85:F6:2D:36:4C:9D:23:99:FB
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
#1: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 22 7A DA 83 AD 16 E2 60 7D C0 82 17 76 9F C1 2C "z.....`....v...
0010: BC DD 41 C0 ..A.
]
]

#2: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:0
]

#3: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Key_CertSign
Crl_Sign
]

#4: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 22 7A DA 83 AD 16 E2 60 7D C0 82 17 76 9F C1 2C "z.....`....v...
0010: BC DD 41 C0 ..A.
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
C:\Program Files\Java\jre1.8.0_111\bin>

```

Verify the new Java keystore's details by running the following command if required;
keytool -list -keystore c:\Certificates\OPI_PSP_1Root

```

C:\Program Files\Java\jre1.8.0_111\bin>keytool -list -keystore c:\Certificate\OP
I_PSP_1Root
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

myrootca, 23-Nov-2016, trustedCertEntry,
Certificate fingerprint (SHA1): E0:78:6D:D7:B6:CB:68:0D:33:6E:0A:FD:86:0E:D1:CA:
28:19:D0:D5

C:\Program Files\Java\jre1.8.0_111\bin>

```

OPI_PSP_1.pfx & OPI_PSP_1Root must be located in the following folder:
 \OraclePaymentInterface\v19.1\Services\OPI\key\

Configuring Token Exchange

1. At OPI Configuration, go to **Token Exchange tab** and set below for SPMS uses :

Figure 3-1 - OPI Configuration Token Exchange

- **Host URL:** The PSP Host URL for Token Exchange
 - **Failover URL:** The PSP Failover Host URL for Token Exchange. If a failover URL is not available, leave this blank
 - **Keystore Password:** Password of the Key Store containing the PSP Root Certificate
 - **Repeat Keystore Password:** Password of the Key Store containing the PSP Root Certificate
 - **Certificate Password:** Password of the Client-Side Password provided by the PSP
 - **Repeat Certificate Password:** Password of the Client-Side Password provided by the PSP
2. Click **Save**.
 3. Click **Sign Out** to close.
 4. Restart the OPI Services.

4

SPMS Configuration

To enable OPI Handling, login to **Administration module**, go to **System Setup** menu, then **Database Parameters**, and set the Parameter value to “**OPI**” under ‘**Not Specified**’ group, **CC Transfer Format**.

OHC OPI Web Service:

Refer to *SPMS Installation Guide Setting Up SPMS Web Server* section at [Oracle Help Center](#) for steps to install OHC OPI Web Services and OHC OPI Daemon Service.

NOTE:

If the SPMS Webserver is installed on a different machine, you need to copy the below two parameters into your `C:\Users\Public\Documents\Oracle Hospitality CruiseOHCSettings.par`, and ensure that there is a new line at the end of the file.

```
[#OPI Interface.Parameter.OPIInterfaceURL=#]
```

```
[#OPI Interface.Parameter.ClientPort=#]
```

OHC OPI Daemon Service Configuration

To configure the Daemon Services, run `C:\OHCOPIDaemonService\OHCOPIDaemonConfigTool.exe` and insert the fields accordingly.

Table 4-1 - OPI Daemon Service Configuration Field

Field	Description
OPI Port No	The OPI Port Number.
SPMS Client Port No	The SPMS Client Port Number.
OPI Key	The Key generated in OPI Configuration – IFC 8 Key.
Merchant ID	The Merchant ID defined in OPI Configuration.

Figure 4-1 - OPI Daemon Log In Window

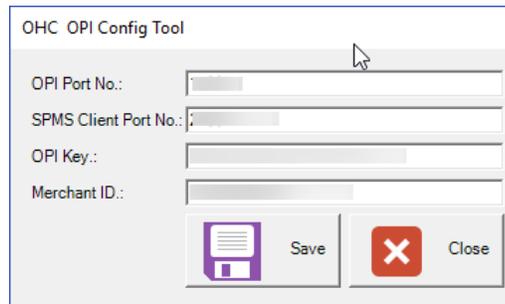
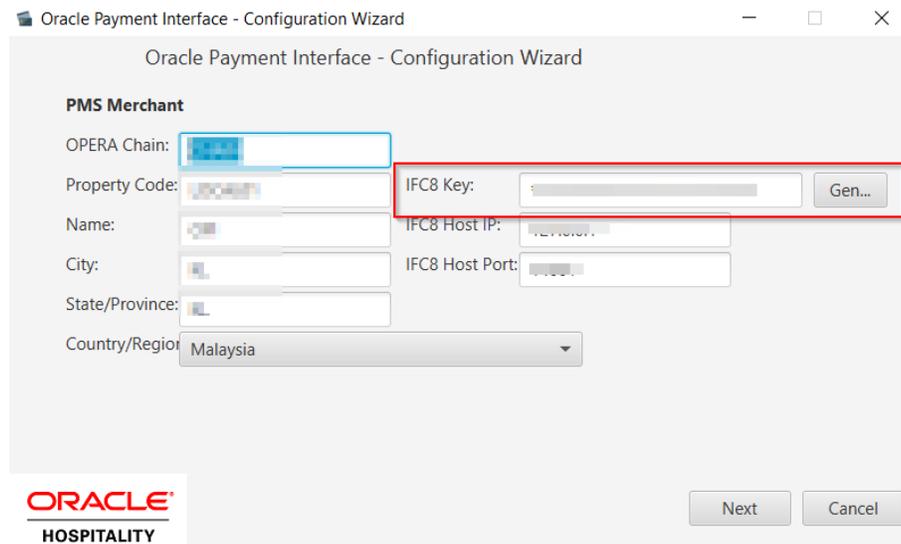


Figure 4-2 - OPI Daemon Service Configuration



OHC OPI Manager

1. Run **OHC OPI Manager.exe** from C:\Program Files (x86)\Oracle Hospitality Cruise.
2. Navigate to **Configuration** tab.
3. Click **Connection** under Setup pane.
4. Enter the following options:

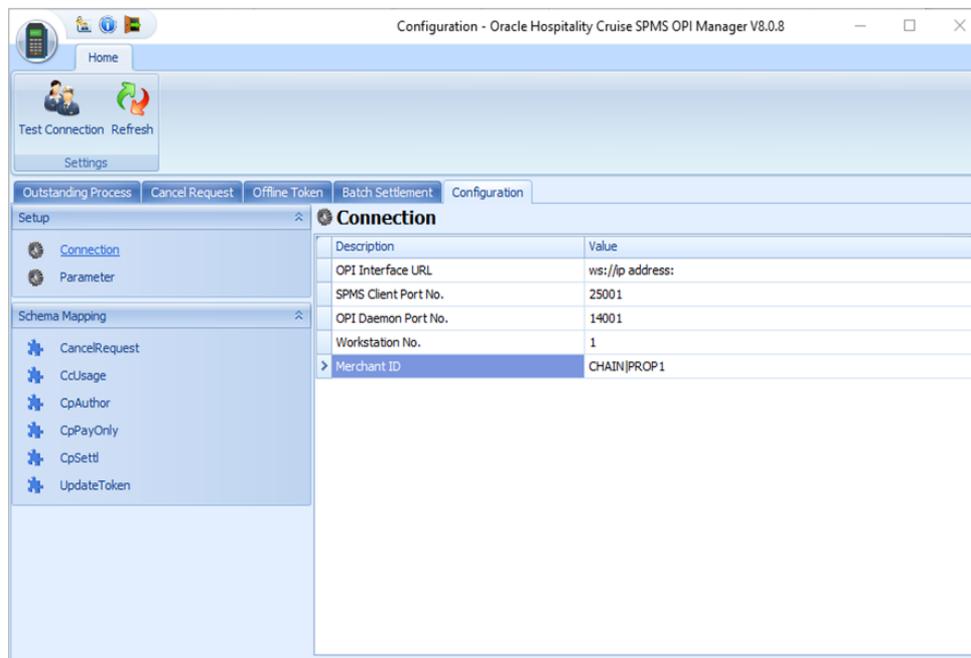
Table 4-2 - OPI Manager Connection Settings

Description	Value
OPI Interface URL	This is where OHC OPI Daemon is installed (in format ws://ip address:)
SPMS Client Port No.	The same SPMS client Port Number that defined in OPI Daemon Config Tool.
OPI Daemon Port No.	The same OPI Daemon Port Number that defined in OPI Daemon Config Tool.

Description	Value
Workstation No.	Workstation Number of the client.
Merchant ID	Combination of OPERA Chain and Property Code values defined in OPI Configuration, for example, CHAIN PROP1.

- Click the **Test Connection** to confirm the connection to OHC OPI Daemon is established.

Figure 4-3 - OPI Daemon Connection Settings



- Click on **Parameter** under Setup pane, select **OPI Web API Service URL** and insert the hostname or IP with port number where the OHC OPI Web Service is installed, for example, <https://localhost:1569/>.